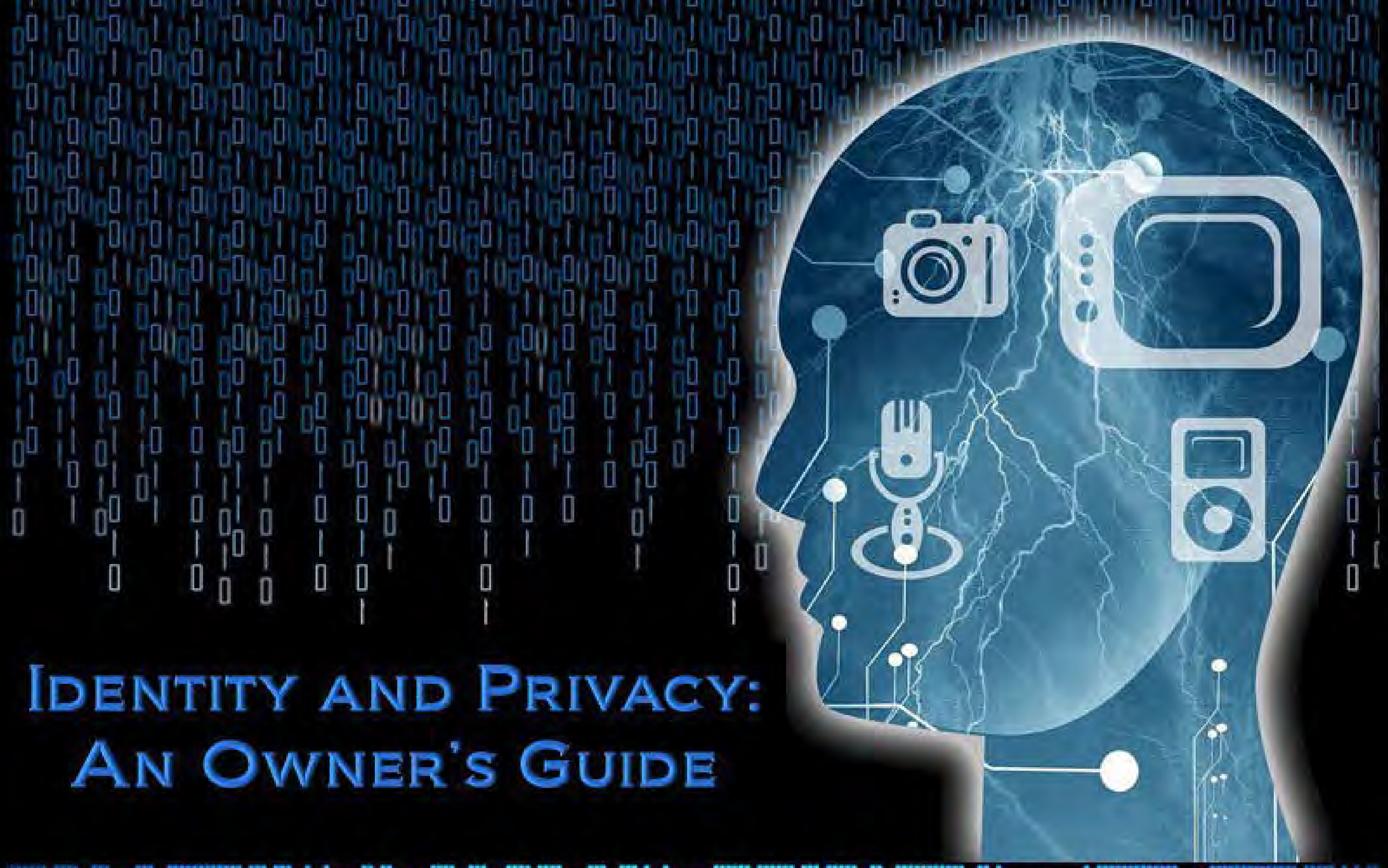
Identity and Privacy: An Owner's Guide



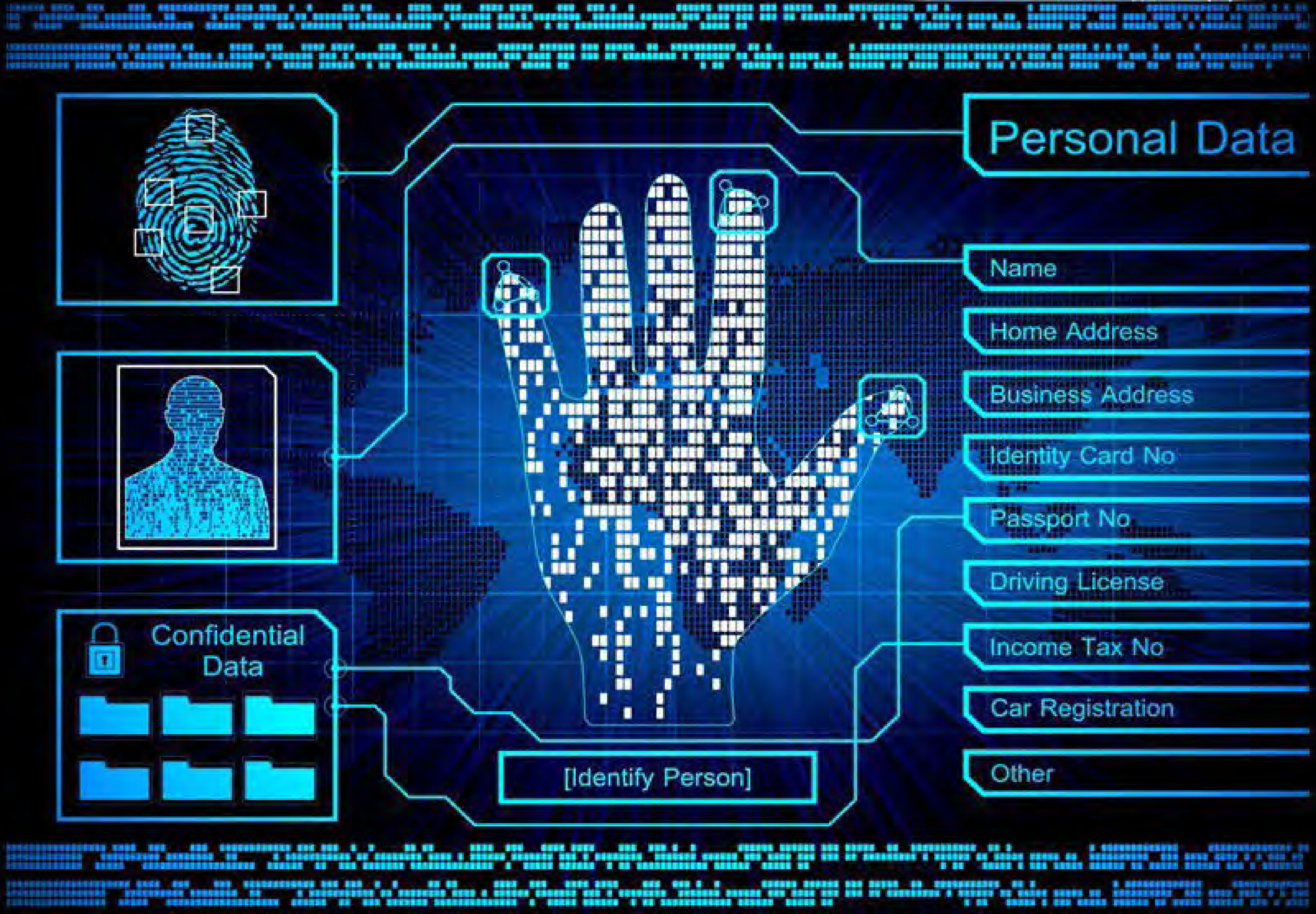
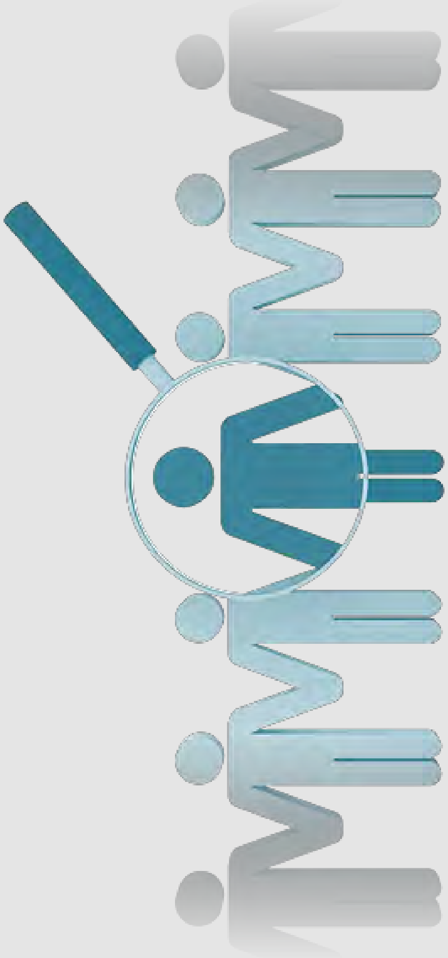


TABLE OF CONTENTS



Err on the side of caution: Assume that the information you post and share is viewable to anyone and everyone.

JANUARY 2021 EDITION

THREATS TO IDENTITY SMARTCARD

THINGS TO CONSIDER ABOUT PROTECTING YOUR IDENTITY

- When buying a new car don't leave all the paper work in the glove compartment or elsewhere in the car . Criminals who break into cars can use that information to steal your identity, not just your car.
- Consider posting travel (vacation) photos and information after you return from your trip so criminals don't know you are away and your house is empty.
- If you are buying or selling something online and it seems too good to be true, chances are it is. A simple Google search of the situation might end up saving you a lot of time and hard earned money.
- Consider turning off your Wi-Fi as soon as you get into your car to leave your house. #habitscanbegood
- Consider how many people have access to public Wi-Fi, then consider only using privately secured Wi-Fi.
- Consider an open-phone policy with your children so you can access their phone anytime and without notice. Remember: if you are "friends" with your kids online that's only half the battle...it's important to check on their accounts to see who and what they are talking about. #keepingourkidssafe
- It's always great to donate, but consider verifying the authenticity of a charity and/or website first. Perhaps visiting an official website or calling the official number.
- Gamers: consider who you are communicating and sharing information with and perhaps limit online gaming interactions to only people you have met face to face.
- Consider logging off of your email and social media accounts when you are not using them, especially on your computer. Doing so will limit the access and abilities of an intruder if they are able to hack in. #protectyourdata

Top Data Breaches of FY 20 That You Should Know

Checking breaches monthly will help to ensure you do not fall victim to identity theft

Instagram, TikTok & YouTube - Aug 2020

Razer (Gaming) - Sept 2020

Acctivision (Gaming) - Possible Sept 2020

Staples - Sept 2020

Barens & Noble - Oct 2020

Mashable.com - Nov 2020

Expedia, Hotels.com & Booking.com - Nov 2020

FireEye - Dec 2020

Spotify - Dec 2020

Microsoft - January 2021

Peekaboo Moments - Jan 2021

THREATS TO IDENTITY SMARTCARD

Useful Resources and Links

https://www.identityforce.com/blog
https://www.commonsensemedia.org/privacy-and-internet-safety
https://www.ftc.gov/
https://identity.utexas.edu/
https://www.getsafeonline.org/
https://staysafeonline.org/
https://www.idtheftcenter.org/
https://www.irs.gov/
https://www.usa.gov/identity-theft
https://www.consumer.gov/articles/1015-avoiding-identity-theft
https://www.transunion.com/fraud-victim-resource/child-identity-theft

What to lock down

- Any PII Information
- Your credit report
- Your child's credit report
- Your social media accounts (recommend utilizing smartcards to lock accounts down)

In Cases of Identity Theft:

- Notify your bank & credit card companies
- Change all passwords including on social media
- Report ID Theft to www.FTC.gov
- Let friends and family know in case the criminal now has access to your emails and social media accounts
- File a Police report

Actions to Take in 2021

- Recommend turning on Two Factor Authentication for all devices and accounts that allow such an option
- Update your devices' virus protection and your passwords
- Clear cookies and browser history frequently
- Update , Update , Update!!! Make sure to allow your device to update to ensure you have the most up to date security measures
- Make sure you backup all your devices.
- Encrypt your emails
- Never save credit or debit card information to devices, apps, or accounts for quick and easy checkout
- Verify those emails; most official business emails will not ask for your PII or Password...check those links
- Don't accept friend requests from strangers
- Consider using a VPN

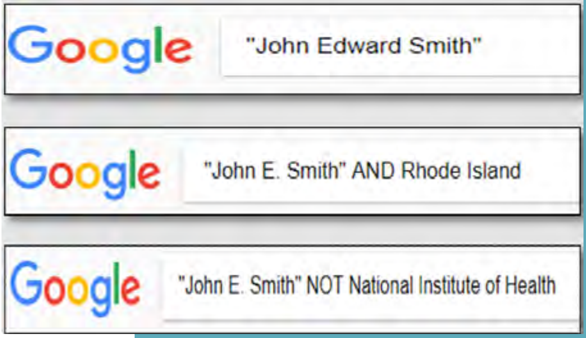
- **Actions for the Physical World**
- Be aware of your surroundings
- Invest in a home safe
- Shred documents, bills, and any mail
- Do not give out your SSN
- Be mindful of shoulder surfers (whether on your phone, computer, at an ATM, etc.)
- Be mindful of credit card skimmers at ATMs and Gas pumps
- Use a locked mailbox
- Check financial statements frequently
- Read medical statements
- Use credit cards instead of debit cards
- Be sure to sign the back of any credit or debit card

Note: Be sure to check out https://haveibeenpwned.com/ to see if your personal data, via your email address, has been compromised in any data breach. Not all data breaches are included on this website but it's a great start to owning your Identity.

HOW TO CONDUCT A SELF ASSESSMENT

Your Online Presence

One of the easiest ways for people (e.g. potential employers, criminals, etc.) to get information about you is through your existing online presence. There, they can learn about you with just a few clicks of the mouse and a quick Internet search. It is therefore important for you to know just what is out there publicly available about you, and how you might reduce any unwanted information.

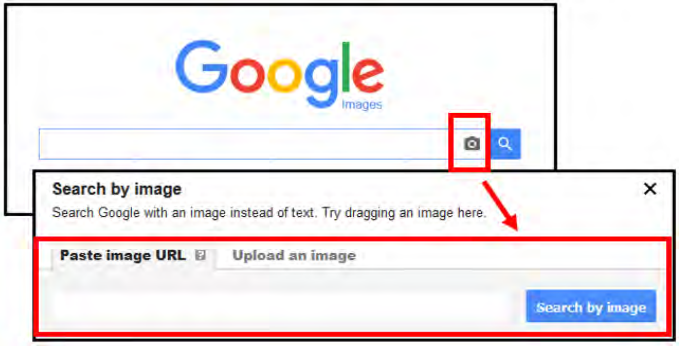


"John Edward Smith"

"John E. Smith" AND Rhode Island

"John E. Smith" NOT National Institute of Health

Review your social media accounts and available data aggregator websites to determine what, if any negative or unwanted information is out there about you. Remember, your close contacts, including family members may have also, unintentionally exposed information about you. It is important to also review what others may have posted about you especially if you have been tagged, directly linking you to a post and making you much easier to find.



Search by image

Search Google with an image instead of text. Try dragging an image here.

Search Engines

Search yourself using various search engines such as Google, DuckDuckGo, etc. for the differences and benefits of each (for a few examples of popular search engines please see the third page). Please note that Google appears to yield the most accurate results for people searches and captures more relevant information.

Prior to researching, ensure you are not logged into any of the search engine sites such as Google or Yahoo. Be sure to delete your browser history and clear cookies before you begin and when you have completed all your research.

These next instructions are related to the Google search engine, but can be applied to most other search engines.

Start with basic personal information such as First and Last Name. If you have a common name, you may want to search First, Middle, and Last Name, or your name associated with a City and State, Home Address, or an associated organization. Please see the examples to the left.

Please note that search terms within quotations marks “ ” will yield results that have the same terms in the same order as the ones inside the quotes. So “John Edward Smith” will not necessarily return the same results as “Edward, John Smith.”

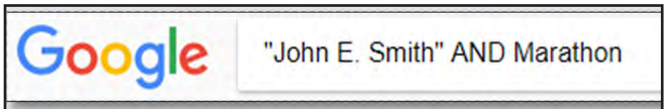
Google does support Boolean logic, however you might, instead decide to use its own search operators which can be found here: https://support.google.com/websearch/answer/2466433?hl=en

You will also want to search your email addresses, usernames, and phone numbers within quotation marks.

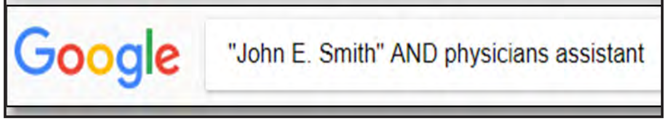
If your search results continue to include items that are not relevant, use the dash sign to exclude certain search terms like this: “John Smith” -Pocahontas

You may want to conduct an image search on any photos you have used as profile pictures on social media accounts or posted to other places online. The reason for this is to ensure that advertisers and/or any other company or individual hasn't taken your picture for their own personal use. To conduct an image search using Google, go to images.google.com, click the camera icon, then select Upload an image. Select the image you want to use to start your search.

Collectively the search engine results will give you an idea of the information that can be quickly collected on you. For example, you may have found and information about previous work experience, hobbies (e.g. races, sporting events), or schools (e.g. graduation announcement). Use that information to conduct further searches such as the example shown to the left.



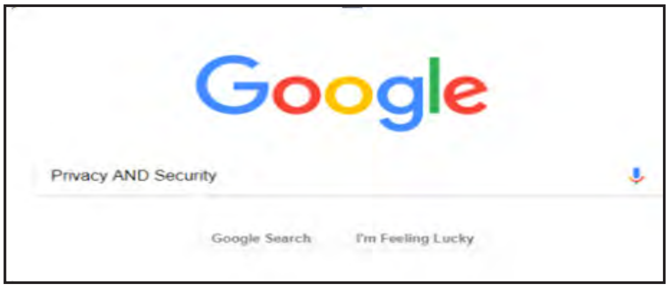
"John E. Smith" AND Marathon



"John E. Smith" AND physicians assistant

Boolean Match Logic

Boolean Search is a way to organize your search using a combination of keywords and the three main Boolean operators (AND, OR and NOT), to produce more accurate and more relevant results See the example to the left. Other helpful operators include " " and ( ).



Privacy AND Security

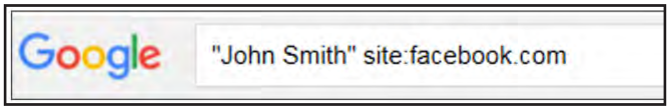
Social Media Search

Take an inventory of the social media accounts that you currently maintain. Some examples include, Facebook, Instagram, LinkedIn, Twitter, etc. First, without being logged in to any social media accounts, conduct open source searches on yourself to see what is viewable to the public. Remember, if your social media accounts don't show up during your open source searches that doesn't mean your account is completely private. It's important to check out the smartcards to help you lock down your accounts to your own personal satisfaction.

Next, login to those accounts and thoroughly review your profile for sensitive information and consider removing unnecessary data:

> Review your profile to see what data is available to the public (address, employment, phone number, etc.)
>
> Check any photos that you have posted or have been tagged in (this can be done through your Activity Log if using Facebook)

* See Facebook, Instagram, Twitter and LinkedIn Smart Cards to learn how to properly set privacy settings.



"John Smith" site:facebook.com

Additional Examples of People Finder Open Source/Fee Required Sites

www.truthfinder.com
www.findpeoplesearch.com
www.privateeye.com
www.peoplefinders.com
www.usa-people-search.com
www.spokeo.com
www.locateplus.com
www.peekyou.com
www.thatsthem.com
www.familytree.com
www.instantcheckmate.com
www.zabasearch.com
www.publicrecords.com
www.whitepages.com
www.reversegenie.com
www.yasni.com

Cont. on page 4.

Note: If you post something on your social media account, it may show up on search engine search results. Remember to set your privacy settings.

People Finder Open Source/Fee Required Sites

Conduct searches on various data aggregator sites. Examples include:
www.ussearch.com
www.spokeo.com
www.beenverified.com
www.intelius.com
www.radaris.com

You can conduct an initial search for free, but all of these sites require payment to access a full report. These sites require no special authorities; anyone with Internet access and a credit card can purchase reports, so it is a good idea to be familiar with the information that can be discovered through them.

If you find information that you do not want publicly available in any of the reports, contact the organization to request that your information be opted out.

Once you've opted out of or suppressed any sensitive information you have found, consider setting up Google Alerts so that you're notified if the information reappears.

Relatives

Though you may have found most of your information conducting your individual search, it might be a good idea to conduct a light search on friends and family members. Remember, they may have posted information about you that an adversary may be able to access.

- Ensure nothing posted on any of the accounts indicates or outright displays personal information you don't want discovered.
- Ask immediate family members (spouse, children, etc.) to review their account settings and postings to ensure that they have not inadvertently posted personal information about you or themselves.
- Provide family and friends with copies of our Smartbook or Smart Cards to help them with locking down their accounts and devices.

Examples of Common Search Engines

www.google.com

Google is a search engine that specializes in Internet-related services and products. These include online advertising technologies, search, cloud computing, and software. The majority of its profits are derived from AdWords, an online advertising service that places advertisements near the list of search results.

www.bing.com

Bing is the second largest search engine in the U.S. Searches conducted using Bing generally yield similar results to Google, however Bing's image search capability (https://www.bing.com/images) is considered superior by most.

www.duckduckgo.com

DuckDuckGo is a search engine that distinguishes itself from other search engines by not profiling its users and by deliberately showing all users the same search results for a given search term. Does not store or compile any of your data to include searched data or personal information (meaning it will not learn from your searches in the same way that Google will). DuckDuckGo emphasizes getting information from the best sources rather than the most sources, generating its search results from key crowdsourced sites such as Wikipedia and from partnerships with other search engines like Yandex, Yahoo!, Bing, and Yummly.

www.searx.me

Searx is a metasearch engine, aggregating the results of other search engines while not storing information about its users.(2)

https://archive.org

The Internet Archive is an American digital library with the stated mission of "universal access to all knowledge." It provides free access to collections of digitized materials, including but not limited to; websites, software applications, music, videos, moving images, and millions of public-domain books.

Examples of Common Social Media Sites

www.facebook.com
www.linkedin.com
www.myspace.com
www.twitter.com
www.tumblr.com
www.classmates.com
www.instagram.com
www.vk.com
www.pinterest.com
www.flickr.com
www.meetup.com
www.youtube.com
www.snapchat.com
www.reddit.com
www.tiktok.com

Additional Examples of People Finder Open Source/Fee Required Sites

www.social-searcher.com
www.infospace.com
www.lullar.com
www.publicrecordsnow.com
www.findoutthetruth.com
www.truepeoplesearch.com
www.checkpeople.com
www.peoplelooker.com
www.persopo.com
www.peoplefinder.com
https://carsowners.net
https://allpeople.com

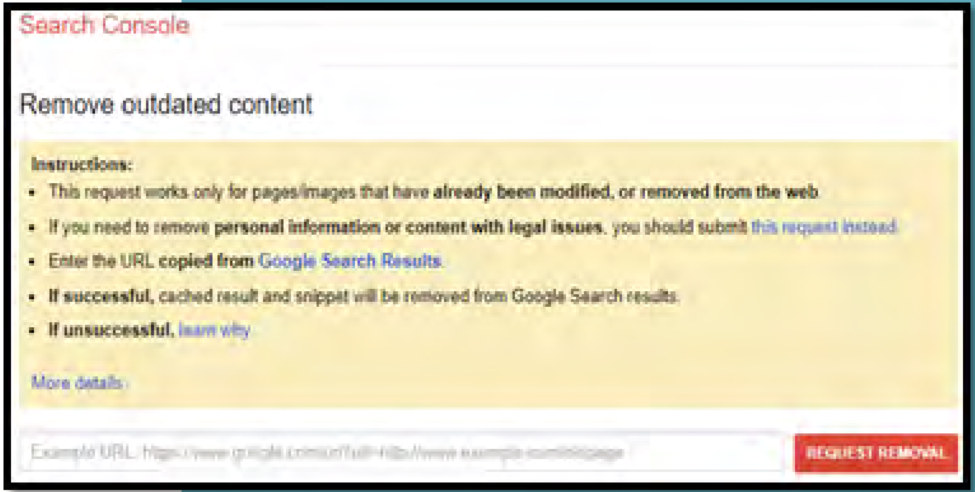
Search Engine Opt Out

Google

https://www.google.com/webmasters/tools/removals

While conducting a "Self Assessment" (see the Self Assessment card) you may find Google Search Results (websites) that you wish to remove.

Find the URL associated with the "Search Result" you wish to remove and paste the URL in the "Request Removal" box (see URL above and picture to the right).



Search Console

Remove outdated content

Instructions:

- This request works only for pages/images that have **already been modified, or removed from the web**
- If you need to remove **personal information or content with legal issues**, you should submit this request instead
- Enter the URL **copied from** Google Search Results
- **If successful**, cached result and snippet will be removed from Google Search results.
- **If unsuccessful**, learn why

More details

Example URL: https://www.google.com/url?url=http://www.example.com/mypage

It is important to note that a "Search Result" cannot be removed so long as the information and URL remain active on the original Webmaster's page. In order to remove your information from Google you must first contact the Webmaster where the information resides and ask that it be removed. Once you obtain confirmation that the information has been removed, you can then "Request Removal" from Google.

On the "Search Console" page, you can also track you requests to determine if Google has accepted the removal request.

Bing

To remove a search result or cache from Bing, go to the above URL and follow the steps located on the Bing website, under "Removing Outdated Cache".

Like any search engine, it is important to note that your information cannot be removed from Bing prior to it being removed from the active website via the websites Webmaster. You will also need to create and sign into Bing with your Microsoft account (formerly Windows Live ID) in order to submit your request and track its progress.

Acxiom

What kind of books do you read? What kind of shoes do you buy? What type of information do Marketers have on you?

Acxiom Corporation is a database marketing company. The company collects, analyzes and sells customer and business information used for targeted advertisements. Good news! Opt Out of this service simply by following the link shown above. #protectyourdata

Google Analytics Opt Out

To provide website visitors the ability to prevent their data from being used by Google Analytics, they have developed the Google Analytics opt-out browser add-on for the Google Analytics JavaScript (ga.js, analytics.js, dc.js).

If you want to opt-out, download and install the add-on for your web browser. The Google Analytics opt-out add-on is designed to be compatible with Chrome, Internet Explorer 11, Safari, Firefox and Opera. In order to function, the opt-out add-on must be able to load and execute properly on your browser. For Internet Explorer, 3rd-party cookies must be enabled.

BeenVerified

BeenVerified provides a quick and easy process to allow you to remove your information from their People Search results. Using the above link, you can search their database, select your record, and verify your request to opt out by clicking on the link in their verification email. After you verify, they will send you an email confirming that the record you selected has been opted out and will instruct their data partners not to return the record in future People Search results.

BeenVerified uses your email address to send you an email to verify your request to opt out. They will not sell the email address that you provide as part of the opt-out process, or use it for any other purpose, without your prior consent. There is no charge to remove your data from BeenVerified's People Search results. Once you receive their email confirming that they have processed your opt-out request, your request will be reflected in their People Search results the next time their server refreshes. In most cases, this will take 24 hours to take effect and then they encourage you to check for yourself.

Once you receive their email confirming that they have processed your opt-out request, your request will be reflected in their People Search results the next time their server refreshes. In most cases, this will take 24 hours to take effect and then they encourage you to check for yourself.

Once your opt-out has been processed, they will instruct their data partners not to return the record you opted out in future People Search results. At this time, they only provide an opt-out for their People Search service. Therefore, it is possible that your name will appear in search results for the other search services available through BeenVerified even after you opt out of People Search.

There may be times when one of their data partners provides a new record that is different enough from your existing, opted out record that they cannot match this new record to the existing record opted-out record and will create a new one. Accordingly, if you have previously opted out and see a new record about you appear in their People Search results, contact them at privacy@beenverified.com and they will help you remove that record as well. It is important to occasionally check BeenVerified to ensure the opt-out process is continuing.

People Finders

https://www.peoplefinders.com/manage

Upon request, Peoplefinders can block the records they have control over in their database from being shown on PeopleFinders.com. Unless otherwise required by law, they will only accept opt-out requests directly from the individual whose information is being opted-out and they reserve the right to require verification of identity and reject opt-out requests in their sole discretion. Of course, they are unable to remove any information about you from databases operated by third parties. They do not accept opt-out requests via fax or mail.

They are not obligated by law to block the records they have control over in their database from being shown on PeopleFinders.com. Despite this, they will endeavor to comply with any such requests to block the records they have control over as described above. Please note, they have no control over public records, and do not guarantee or warrant that a request for removal of or change to personal information as described above will result in removal of or change to all of your information from PeopleFinders.com. Further, they are not responsible for informing third parties with whom they have already shared your personal information of any changes. Just because PeopleFinders.com is associated with a separate aggregator does not mean they will contact them on your behalf to remove your information you must visit each site.

Individual Data Aggregator Removal Links

PrivateEye, Veromi, PeopleFinders, and PublicRecordsNow are all owned by the same parent company, Confi-Chek.com. You must still opt out of each individually.

- Opt out of PrivateEye by completing the form at:
- https://www.privateeye.com/static/view/optout/
- Opt out of Fastpeoplesearch by completing the following steps at: https://www.fastpeoplesearch.com/removal and by visiting the Peoplefinders opt out (url below).
- Opt out of PeopleFinders and Public Records Now by visiting: https://peoplefinders.com/manage/
- Opt out of USA People Search by visiting:
- https://usa-people-search.com/manage

Radaris

To opt out of Radaris follow the instructions at: http://radaris.com/page/how-to-remove

Group Removal Data Aggregator Links/Information

Intelius owns, or is affiliated with, the below sites. When you request removal of your records, also request removal from this network of sites. Opt-out of Intelius online at https://www.intelius.com/optout. Of the Intelius affiliates, the following require a separate opt out process where you must fax your ID and a letter containing the information you want removed to 425-974-6194: Peoplelookup, and Phonesbook

Use the following language on the coversheet:

"As per your privacy policy, please remove my listing from iSearch, ZabaSearch, Public Records, People-Lookup, PhonesBook, LookupAnyone, and all other affiliated people search sites. Thank you for your help with this personal security issue."

US Search/Spock/Lookupanyone

Opt out of US Search by visiting https://www.intelius.com/opt-out/submit/. Search for your name and click on the appropriate listing. Print the cover sheet and mail or fax a state issued ID or drivers license to the listed address or fax number. http://www.ussearch.com

Family Tree

FamilyTreeNow allows you to opt out at: https://www.familytreenow.com/optout. The entire process takes place in four simple steps, where you must first select your record and then verify it is in fact your record. After you have found and confirmed your record, you simply click "Opt-Out" and you will have completed the process.

It is important to note that if you found your FamilyTreeNow record on a search engine like Google, FamilyTreeNow has a process for its remove, which can also be found using the link above where you will find additional information under "Notes".

Search for your name, names of family members, email addresses, phone numbers, home addresses, and social media usernames using some of the data aggregator links below. Once you have reviewed your information and identified what needs to be removed (if any), you should record your findings to facilitate the removal process. Please note, the information presented here about how to remove personal details from data aggregators is subject to change. Opting out will not remove your information indefinitely.

TruePeopleSearch

To opt out of TruePeopleSearch simply go to: https://www.truepeoplesearch.com/removal and follow the three step process.

WhitePages

To opt out of Whitepages, search for your information using your first name, last name, city, and state. Once you have located your record copy the URL and paste it here, https://www.whitepages.com/suppression_requests/. Next, follow the steps to complete the removal process. This process will require a phone call from WhitePages (computer generated) in order to complete the process.
http://www.whitepages.com

MyLife

Call MyLife at 888-704-1900. Press 2 to speak to an operator. Tell the representative that you want your listing removed and provide the information you want deleted. A second option is to request opt out via email at: privacy@mylife.com. Be sure to specifically request your information is removed from Wink.com as well as MyLife.com. Once they confirm the removal, the listing will be off the site in 7-10 days. http://www.mylife.com

Been Verified

BeenVerified allows you to opt out at https://www.beenverified.com/faq/opt-out/. Search for your listing and claim it by selecting the ">" on the right side of your record . Enter your email address. You must click the opt out link within the email sent to your account.

PeekYou

To opt out of PeekYou, fill out the form at: http://www.peekyou.com/about/contact/optout/index.php. Select Remove my entire listing under Actions. Paste the numbers at the end of your profile's URL in the UniqueID field. Fill in the CAPTCHA, and you're all set. You'll get an immediate email confirming you've sent in your opt out form and a second email in a few days or weeks to tell you that it has been deleted. http://www.peekyou.com

USA People Search

To opt out of USA People Search, go to https://www.usa-people-search.com/manage/ and search for your information. Once you have located your record select "That's the One." The next page will be a confirmation that you would in fact like to Opt Out of the USA-people-search database, click the agreement blocks at the bottom of the page and it will complete the Opt Out Process

.

InstantCheckMate

To opt out of InstantCheckMate, follow the instructions at:
http://instantcheckmate.com/optout
You can opt out by mail or online.
You must provide them an email address to send the record removal to.

- Conduct research to see what records data aggregator has collected about you.
- Some data aggregators may have information about you and your family under multiple listings; you may need to repeat the removal process described below for each listing.
- Follow ALL necessary steps to complete the removal process; you may need to mail or fax information to the aggregator.
- Understand that incorrect information may be a good thing and that it might not be necessary to "fix".
- Do not think removing your information from data aggregators will suppress everything. Information in data aggregators about family members may still contain information about you.
- Don't think you have to delete all your information on these sites. Some information on data aggregator sites is "normal."
- Do not remove information on other family members. If there is information that you believe is harmful to you, contact your family member and help them to go through the removal process.

GOOGLE ALERTS SMARTCARD

HOW TO SET UP GOOGLE ALERTS

BACKGROUND

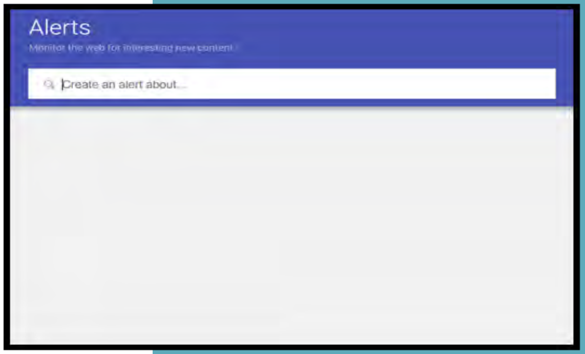
Google Alerts is a free Google feature that monitors the internet for mentions of any topic a user specifies. Google collects and packages all instances of these mentions and delivers them to the user continuously (as soon as Google recognizes the mention), daily or weekly. For instance, you may choose to be notified anytime your name is mentioned in an article, when a specific job title is posted, or when your business is mentioned.

Step 1: Open the Website

To begin, type "Google Alerts" into your search engine, or you can go directly to the website http://www.google.com/alerts. It might be helpful to bookmark this page for easier access in the future..

Step 2: Enter Your Search

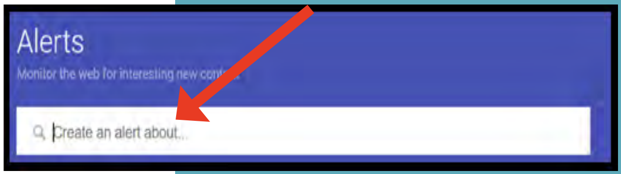
Under "Alerts" (highlighted below), enter the topic you would like to receive alerts about. As soon as you begin typing, a sample of your first alert will appear. If you are not getting the results you want, you can change your input right away. You may decide to set an alert for your own name to help monitor what might be out on the internet about you, especially after you have reviewed the "Self-Assessment card".



Alerts

Monitor the web for interesting new content

Create an alert about...



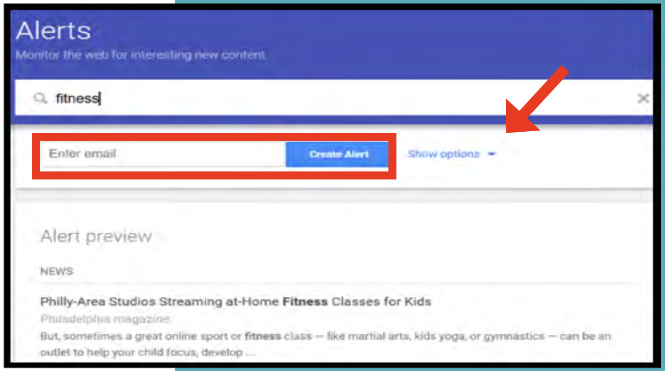
Alerts

Monitor the web for interesting new cont

Create an alert about...

Step 3: Create the Alert

Enter a valid email address, where Google will send you the results of your query. Then complete the process by clicking on the "Create Alert" button. (If it doesn't ask for your email, you are likely already logged into your Google Account, and will receive the emails in the associated email account). You will receive an email from Google Alerts asking you to confirm or cancel this request. Once you confirm the request, you will begin receiving your alerts. Your first basic Google Alert is now complete. See Step 4 to learn how to further specify search parameters.



Alerts

Monitor the web for interesting new content

fitness

Enter email | Create Alert | Show options

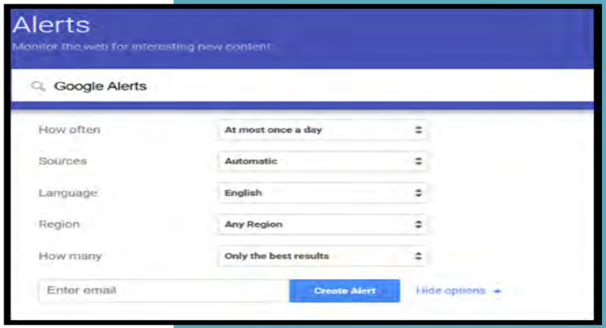
Alert preview

NEWS

Philly-Area Studios Streaming at-Home **Fitness** Classes for Kids

Philadelphia magazine

But, sometimes a great online sport or **fitness** class — like martial arts, kids yoga, or gymnastics — can be an outlet to help your child focus, develop ...



Alerts

Monitor the web for interesting new content

Google Alerts

How often	At most once a day
Sources	Automatic
Language	English
Region	Any Region
How many	Only the best results

Enter email | Create Alert | Hide options

Step 4: Choose Search Parameters

Select "Show options" to adjust:

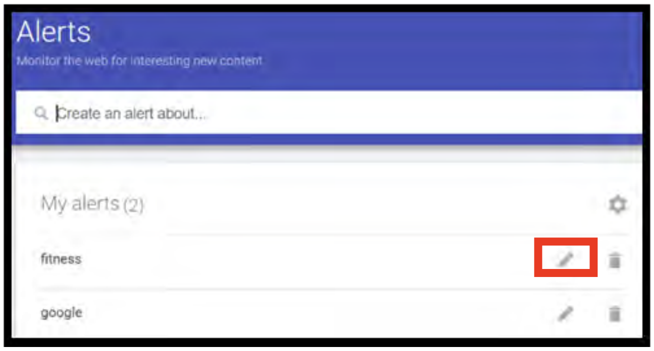
- How often you want to receive alerts (choose as it happens, once per day, or once per week)

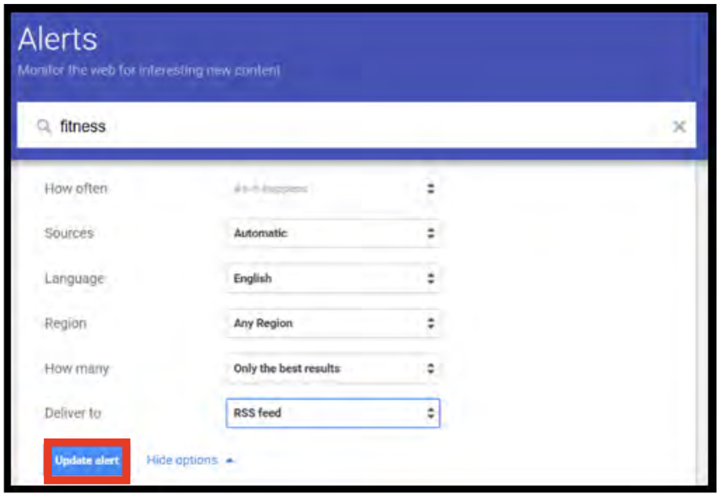
Tip: You can use the search box like you would in Google Search, but avoid general terms or the vast majority of the results will be wildly unnecessary and difficult to sift through. You can use advanced search commands, surround the search in quotes for phrase searches, search on a specific site only, etc.

- The source of the search (e.g., Video, News, Web, Books)
- The language of the source website
- The region in which the search should take place (like the U.S., Egypt, Spain, etc.
- How many search results you want to see (only the best results or all search results)
- Where to deliver the Google Alerts data (your email address or an RSS feed)

Modify Alerts

If you would like to modify your current alerts complete the following steps. Select the "Edit" button next to the alert you wish you modify (see the Pencil icon as highlighted below). You may now change the alert keywords, as well as any of the search parameters listed. To finish, select "Update alert" at the bottom.

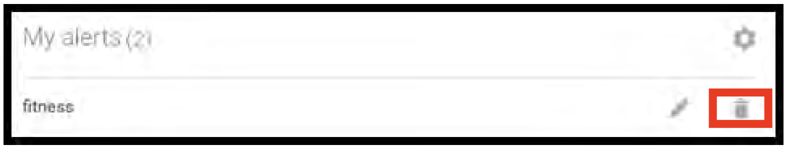




How often: As-it-happens
Sources: Automatic
Language: English
Region: Any Region
How many: Only the best results
Deliver to: RSS feed

Delete Alerts

If you ever wish to delete one or more of your alerts, you can do so easily by clicking the "Trash can" icon next to the alert you wish to delete..



> **"Google Alerts are a simple and free way to monitor what's going on in your industry…You should also be monitoring your name and business name, that way you know if people are talking about you, your company, and your brand."**
>
> **Michelle Arbore, Savvy Social Media**

Tip: Emails from Google Alerts are sent from googlealerts-noreply@google.com. You might set up an email filtering rule for messages from that address so that they're sorted into a special folder instead of in your inbox, where they can easily cause cluttering.

ONLINE REGISTRATION SMARTCARD

Identify Elements of Social Networking Site (SNS) Accounts

First & Last Name

First and last name are mandatory for almost all SNS accounts. In order to better protect yourself, it is important to make sure your account is locked down and consider having a profile picture that is something other than your photo.

Gender

Gender is a common field to fill out on the registration page, used mostly for future content customization. Whenever possible, avoid making a distinction when signing up for your account. Location: Address, Zip Code, Country

Location

information is required to various levels of granularity depending on the service. It may include address, zip code, and/or country.

Username

Username is unique to each user account, unlike first and last name which can be shared across multiple users. DO NOT include personally identifiable information, such as last name or birthday, when creating your username.

Birthday

Birthdays are used to verify the user's age and customize age-appropriate content for the user on the site. This information is sometimes published on the SNS profile and must be removed retroactively.

Company/Employment Information

Company and employment information are required for professionally-oriented SNS services, where the main purpose is to meet and build your network with other people in your field.

Sexual Orientation/Relationship Status

These fields are most often required in online dating sites, where the main purpose is to meet people.

Mobile Phone Number

Registering for email accounts frequently requires a verifiable phone number. Refrain from using services that require phone numbers or opt to use an alternative method to verify accounts.

Email Address

Email is the 2nd most common requirement for creating a SNS account. It is used to verify your account during registration and often used as a credential for future log-ins.

Online services include sites that require users to register and create personal profiles prior to using their service. Best practices include:

- Review the terms of service for each site to determine their privacy policy and data sharing agreements with third party entities.
- Avoid filling in optional identity fields for online profiles; only fill in the minimum required identity information.
- Never give online services access to your social security number or physical address.
- Turn down options to upload and share your existing contacts during registration.
- Check and, if necessary, change privacy settings to protect your personally identifiable information immediately after completing the registration process.

Online identity can be described as an aggregate of accounts and account-related activities associated with a single person. Common identity elements required by SNS for creating accounts and participating in their online services are shown below.

ONLINE REGISTRATION SMARTCARD

IDENTITY INFORMATION REQUIRED DURING ONLINE SERVICES REGISTRATION

	LinkedIn	Facebook	Twitter	Instagram	Spotify	Amazon	Pinterest
First and Last Name	X	X	X	X	X	X	X
Username	*Uses name by default	x	X	X	Optional	*Uses name by default	*Uses name by default
Password	X	X	X	X	X	X	X
Birthday	X	Optional		Optional	X	Optional	
Gender	Optional	Optional		Optional	X		Optional
Email Address	X	**Optional	X	X	X	X	X
Phone Number		**Optional	Optional	Optional	Optional	Optional	
Country	X	X	X	X	X	X	X
Company/ Employment Info	X						
Job Title	X						
Zip Code	X					X	
Facebook Account	Optional	X	Optional	Optional	Optional	Optional	Optional

*Social media sites default to the "name" provided when settings up the account as your Username, instead of asking Users to create a "handle."

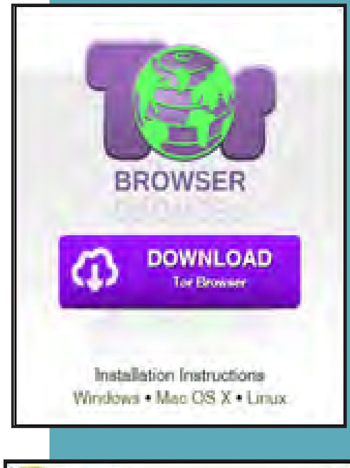
** Facebook requires a mobile number or email address when registering an account. Consider using a Google Voice number for two factor authentication for additional security.

It is a lot easier to simply sign up or register on a social media site when you link other accounts to them. Usually, it is a simple click of the button; however, it is recommended that you DO NOT do this. If someone gains access to your Facebook account and you have signed up for other SM accounts using Facebook, then that likely gives them access to those other accounts as well. Treat SM account creation just like your password; create a new and unique one for each site you wish to sign up for. Additionally, it is always best to use a current email for any social media use. This way, if something were to happen to your account, you're immediately notified and can quickly correct the problem. If you have an email account that you do not check routinely, or that has suffered a major data breach, you might not know if someone hacked into your social media account(s) until it is too late to fix.

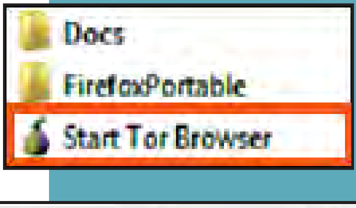
USING TOR TO ANONYMIZE YOUR ADDRESS

Tor Browser is a free, open source web browser that uses a volunteer network of virtual tunnels and a layered encryption process to anonymize your IP address. Note that Tor anonymizes the origin of your traffic and encrypts everything inside the Tor network; however, it cannot encrypt the data after it comes out of Tor at the destination. Tor can be installed according to the instructions to the right.

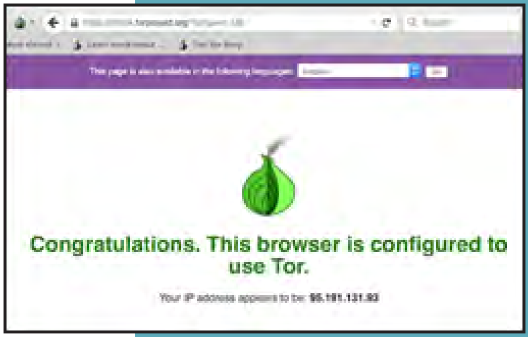
1. Visit torproject.org. Download and Install the Tor Browser Bundle to your hard drive or a flash drive.



2. Launch the Tor Browser which can be found at the location you saved the bundle to. Double-click “Start Tor Browser”.



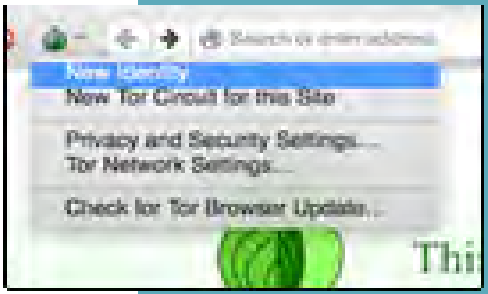
3. Ensure your Tor Browser is providing you with an anonymous IP address.



Congratulations. This browser is configured to use Tor.

Your IP address appears to be: 95.181.131.93

4. To use a new IP address, click the drop down menu ith the onion next to it and select “New Identity”. Please note that doing this will close all of your currently opened tabs.


Search or enter address
New Identity
New Tor Circuit for this Site
Privacy and Security Settings...
Tor Network Settings...
Check for Tor Browser Update...
Thi

Best Practices

- Do always use a secure browser and VPN that anonymizes your IP address when accessing anonymous email services. Be sure your browser is updated regularly.
- Do remember, although the tools anonymize you, if you have to pay with traditional means, you can be identified through that transaction.
- Do use VPN services. They anonymize your IP address, although you will have to submit personal data to sign up for the service.
- Do not access more than one account in a single browser session, and never access popular services such as Google or Yahoo in the same session.
- Do not include personal details in your communication that can be used to identify you, such as your name, phone number or address.
- Do not use anonymous email services on any device that requires personal logins, such as a smart phone with linked accounts.

Warning! Tor is generally used when someone needs to hide their computer’s identity or location. It should not be used as a default search engine for everyday internet browsing. Never visit social networking sites or enter any personal data on any website using the Tor Browser — it is poorly regulated and leaves your information extremely vulnerable to theft.

ANONYMOUS INTERNET & MESSAGING SERVICES SMARTCARD

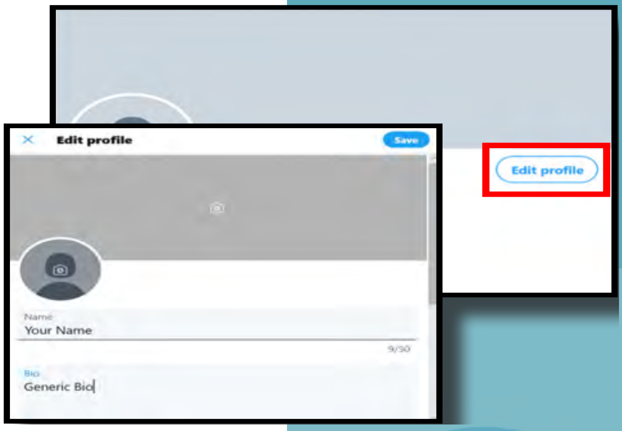
TYPES OF MESSAGING SERVICES AVAILABLE ONLINE

Provider	Service	Primary Use	Data Retained	Data Sharing	Cost
Hide My Ass!	VPN Temporary Email	Freely surf the web (VPN). Receive emails and use the inbox for websites that you do not necessarily trust that require you to provide an email address.	IP address, cookies, payment details, username, password, and actual emails. HMA asks for an existing email address at signup but this is optional.	They do not sell personal data to 3rd parties unless required by law. They do share information with members of AVG Group.	VPN as low as $6.99.
CloakMy	One time message and chat service	One time messaging and chat. You have to send the recipient a unique URL to go retrieve the message.	Logs IP addresses	None, does not share or sell information to others	Email is free.
ProtonMail	End to end encrypted email	Fully encrypted email, emails are encrypted client side so they are fully encrypted when they get to the Proton servers in Switzerland	Optional additional email upon sign up for account recovery purposes.	Proton if compelled, could only hand over encrypted emails. They do not retain the keys to encryption, the client does.	Free
HushMail	Email Host	HushMail is an email host just like Gmail or Yahoo. It is accessible through Tor and it does not require personal information to register.	Browser type, operating system, IP address, credit card information when purchasing product. Retains email messages for up to 18 months, encrypted or non-encrypted.	Logs user IP addresses. They have also turned over user data to U.S. authorities in the past due to court orders.	Free
Signal	Encrypted text messaging	Send one-to-one and group messages, which can include files, voice notes, images and videos, and make one-to-one voice and video calls	Signal users must invite each other using mobile number. The service can encrypt messages but not necessarily anonymize users. The encryption is on the users device rather than the company servers	The messages can be set to self destruct after being read. The app does not retain the message. Signal says it will share information with Third Party service providers, and for legitimate legal purposes.	$49.98/year
Wickr	Encrypted text messaging	End-to-end encryption and content, expiring messages, including photos, videos, and file attachments and place end-to-end encrypted video conference calls	Wickr users must invite each other using mobile number. The service can encrypt messages but not necessarily anonymize users. The encryption is on the users device rather than the company servers	The messages can be set to self destruct after being read. The app does not retain the message	Free
Mailinator	Temporary disposable Email	Use the Mailinator address anytime a website asks for an email address. Can only receive email.	No signup required.	Mailinator is a public domain so anyone can read an email if they know what address was used. Use odd names to avoid heavily used inboxes.	Free

There are many email and messaging options out there that can provide a means to send and receive messages anonymously or semi-anonymously. The right service for you will depend on the primary nature of your communications , the cost, and the information you are willing to provide.

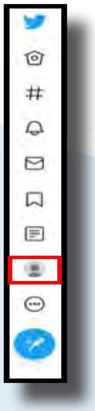
PERSONAL COMPUTER (PC) VERSION

1. Let's start to lock down your account by first checking out what your "Profile" says about you. Click the "Profile" icon at the lower left of the screen — this is likely your profile picture. Click "Edit Profile" as shown to the right.

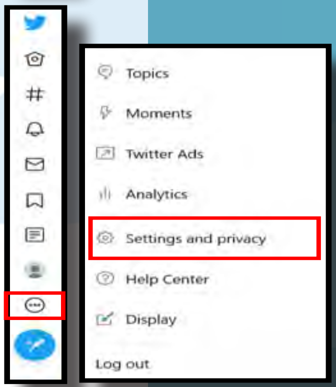


Name
Your Name

Bio
Generic Bio



First, notice the "Profile Image" and "Header Image" sections. We recommend that you do *not* use photos of yourself for your profile and header photos. These are viewable to the public and present an unnecessary vulnerability. Alternative options include avatars and landscape or other types of photos that are not personal and do not contain identifying information within them.



Below the "Profile Image" section are the "Name", "Bio", "Location", "Website" and "Birthday" sections. These are not required to be filled in, and it is recommended that you leave them blank or generic. Even if you use inaccurate location data, it is possible for someone to tie the data back to you by using data aggregator sites. Personally identifiable information (PII) is often used as a means to gain access to certain accounts (banks, credit cards, school etc.). Thus, providing even your birthday could help an identity thief steal your identity.

Now, let's move on to the "Settings and Privacy" tab on the same menu at the left hand side of your screen. (see left) All of these settings need to be separately updated on all the various devices you use to access Twitter, including Android phone, iPhone, and home computers. Twitter is programmed differently on each of these devices, and the settings will not automatically transfer among them. Also, set your "Location" to "Off" on ALL devices.

Do be careful when using #hashtags in Tweets as it allows users to index and associate your Tweet with a particular topic.

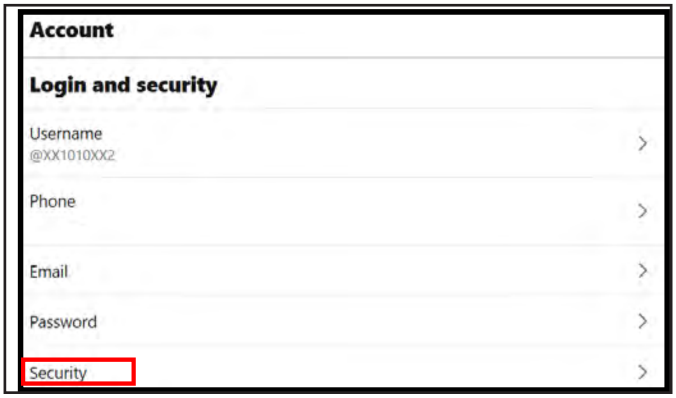
Do ensure that family members take similar precautions with their accounts. Their privacy and share settings can expose your personal data.

Do use caution when posting images and videos of any kind. Be aware of your surroundings, to include identifiable locations and any other personal security vulnerabilities.

Do use a picture of something other than yourself for your profile photo. Profile photos are viewable to the public.

TWITTER SMARTCARD

PERSONAL COMPUTER (PC) VERSION



Account

Login and security

Username
@XX1010XX2

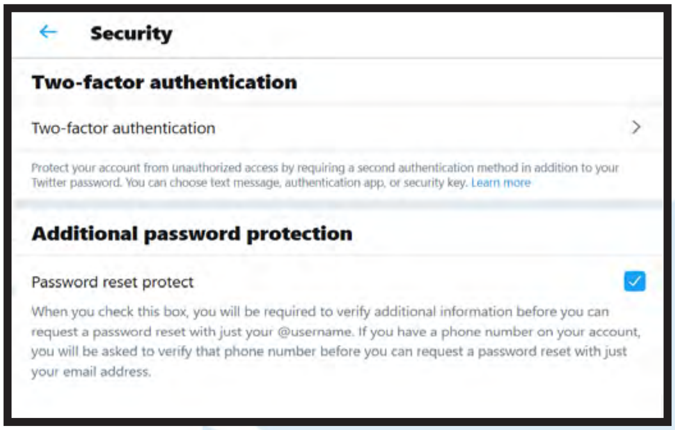
Phone

Email

Password

Security

Once in “”Settings and Privacy” you can review your “Account” information, including “Security” settings and how data, such as your “Username” is displayed. Remember to stop and think about what your “Username” says about you, what is it giving away?



Security

Two-factor authentication

Two-factor authentication

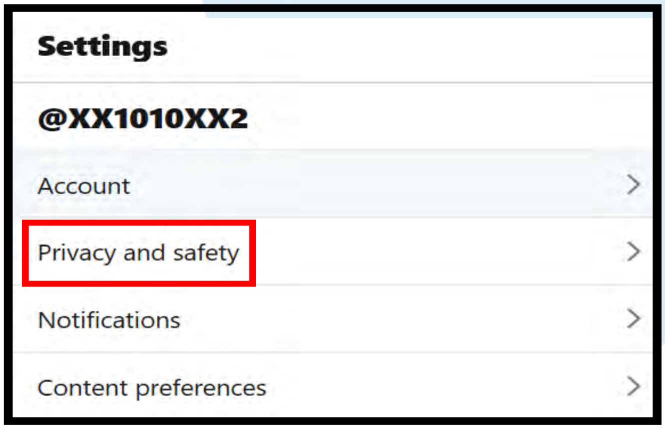
Protect your account from unauthorized access by requiring a second authentication method in addition to your Twitter password. You can choose text message, authentication app, or security key. Learn more

Additional password protection

Password reset protect ☑

When you check this box, you will be required to verify additional information before you can request a password reset with just your @username. If you have a phone number on your account, you will be asked to verify that phone number before you can request a password reset with just your email address.

In the the “Account” section, select “Security”. “Two-factor authentication” is the most secure option, and is recommended for your account. Choose your preferred “Two-factor authentication” option, most likely “Text Message”. Also ensure “Password reset protect” is checked. These settings add layers of protection to prevent your account from being hacked.



Settings

@XX1010XX2

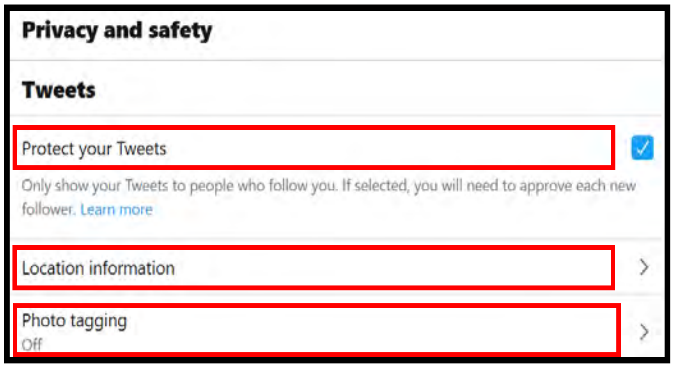
Account

Privacy and safety

Notifications

Content preferences

Next, go back to the left column, under “Settings” and select “Privacy and Safety” (see below). All the sections in RED (below right) are recommended settings that should be selected.



Privacy and safety

Tweets

Protect your Tweets ☑

Only show your Tweets to people who follow you. If selected, you will need to approve each new follower. Learn more

Location information

Photo tagging
Off

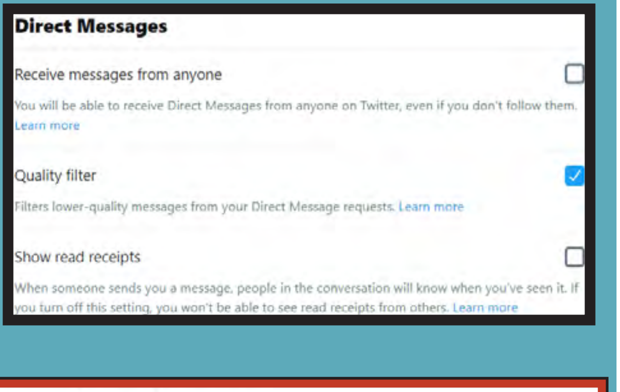
Check the box for “Protect your Tweets”, click on “Location information” and make sure the box on the next screen is *unchecked*. Ensure “Photo tagging” is “Off”. Remember it is always better to control your information than it is to allow someone else to decide for you.

Note: In addition to the information you share with it, Twitter will use your Tweets, content you’ve read, “Liked”, or “Retweeted”, and other information to determine what topics you’re interested in, your age, the languages you speak, and other signals. The purpose is generally to show you more relevant content.

TWITTER SMARTCARD

PERSONAL COMPUTER (PC) VERSION

Let’s scroll to the middle of the page and locate the “Direct Messages” section. *Uncheck* the first and last boxes in this section in order to limit incoming messages from people you do not know.



Direct Messages

Receive messages from anyone ☐

You will be able to receive Direct Messages from anyone on Twitter, even if you don't follow them. Learn more

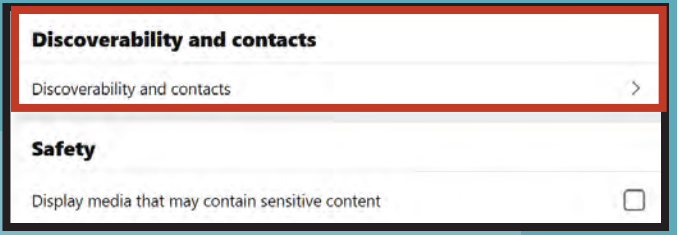
Quality filter ☑

Filters lower-quality messages from your Direct Message requests. Learn more

Show read receipts ☐

When someone sends you a message, people in the conversation will know when you've seen it. If you turn off this setting, you won't be able to see read receipts from others. Learn more

Next is the “Discoverability and contacts section” (see right). Ensure both boxes under “Discoverability” are unchecked. It is best to maintain as much control as possible of who is connecting with you.

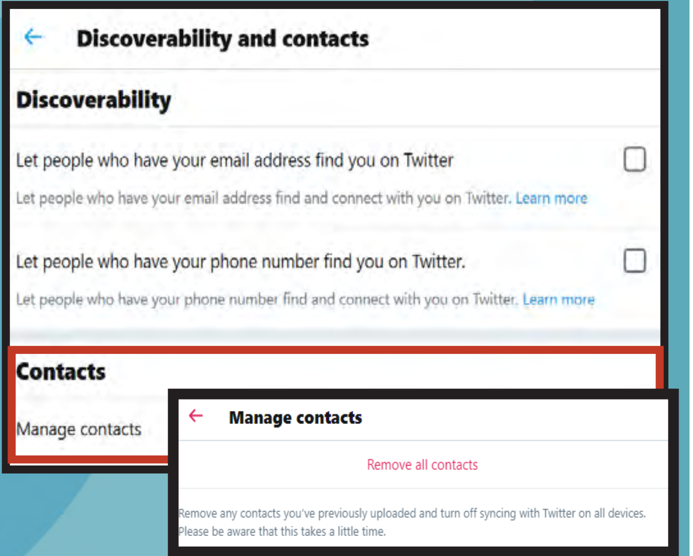


Discoverability and contacts

Discoverability and contacts >

Safety

Display media that may contain sensitive content ☐



← **Discoverability and contacts**

Discoverability

Let people who have your email address find you on Twitter ☐

Let people who have your email address find and connect with you on Twitter. Learn more

Let people who have your phone number find you on Twitter. ☐

Let people who have your phone number find and connect with you on Twitter. Learn more

Contacts

Manage contacts

← **Manage contacts**

Remove all contacts

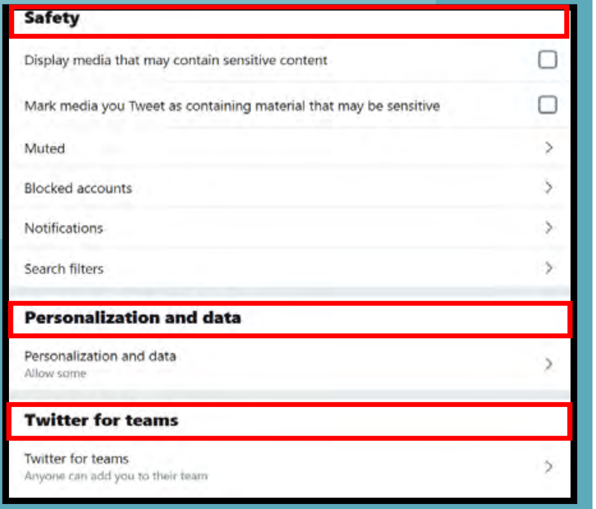
Remove any contacts you've previously uploaded and turn off syncing with Twitter on all devices. Please be aware that this takes a little time.

Now click the “Contacts” section. Here you can review and remove any contacts Twitter has collected. It is recommended that you not synchronize any of your accounts together, to include any email accounts with contact information in them. Synchronizing your email accounts allows Twitter to do more than just upload your contacts — Twitter uses the information to learn more about you and your contacts

.

You should not synch accounts, “Remove all contacts,” if there are any in this section, and remember to keep your identifying information off your own Twitter account, in case your contacts try to import your data to any of their accounts.

Below the “Discoverability and contacts “section is the “Safety” section (left). You may want to review this section in order to better control the types of content you see, and more importantly to control what is displayed on your *child’s Twitter* account.



Safety

Display media that may contain sensitive content ☐

Mark media you Tweet as containing material that may be sensitive ☐

Muted >

Blocked accounts >

Notifications >

Search filters >

Personalization and data

Personalization and data >
Allow some

Twitter for teams

Twitter for teams >
Anyone can add you to their team

#TheMoreYouKnow

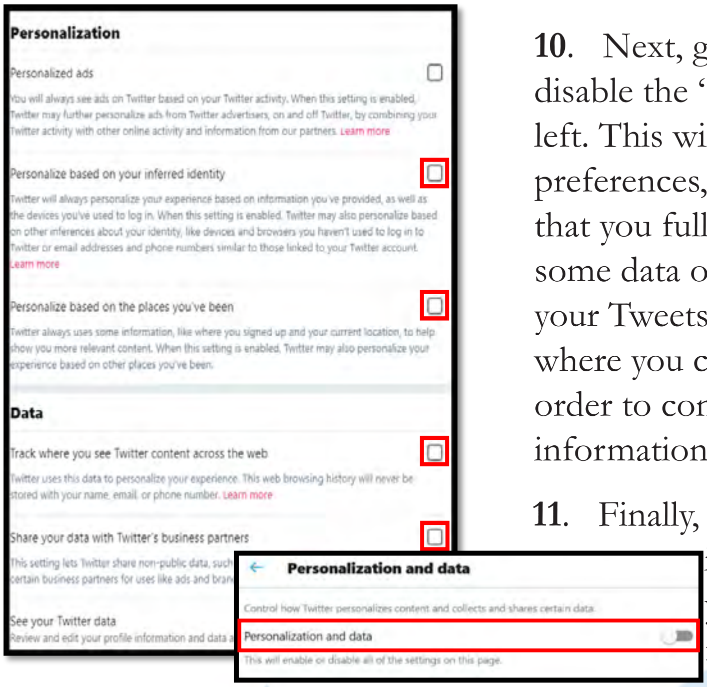
#dataprivacy

#DataSecurity

#identitytheft

Hashtags # are used to index key words and topics on Twitter, think of them as the topic of your “tweet” or “post”. Understand that if your account is public and you use a hashtag on a tweet, anyone who does a search on that hashtag may find your tweet. When you add a hashtag to a tweet, Twitter adds the message to the hashtag group so more users see your “tweet”.

10. Next, go to the "Personalization and data" section and disable the "Personalization and data" switch, as shown to the left. This will stop Twitter from collecting data regarding your preferences, locations, behaviors and activities. We ecommend that you fully disable this function. Twitter will always collect some data on you from your account, for instance based on your Tweets, comments, and engagements within the app. But where you can limit such collection, it is advised that you do, in order to control as much as possible, the extent to which your information is passed around the Internet.



Personalization

Personalized ads ☐

You will always see ads on Twitter based on your Twitter activity. When this setting is enabled, Twitter may further personalize ads from Twitter advertisers, on and off Twitter, by combining your Twitter activity with other online activity and information from our partners. Learn more

Personalize based on your inferred identity ☐

Twitter will always personalize your experience based on information you've provided, as well as the devices you've used to log in. When this setting is enabled, Twitter may also personalize based on other inferences about your identity, like devices and browsers you haven't used to log in to Twitter or email addresses and phone numbers similar to those linked to your Twitter account. Learn more

Personalize based on the places you've been ☐

Twitter always uses some information, like where you signed up and your current location, to help show you more relevant content. When this setting is enabled, Twitter may also personalize your experience based on other places you've been.

Data

Track where you see Twitter content across the web ☐

Twitter uses this data to personalize your experience. This web browsing history will never be stored with your name, email, or phone number. Learn more

Share your data with Twitter's business partners ☐

This setting lets Twitter share non-public data, such
certain business partners for uses like ads and bran

See your Twitter data
Review and edit your profile information and data a

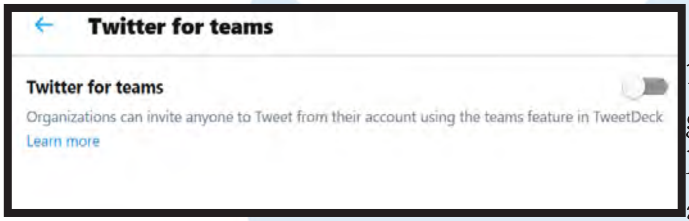
← **Personalization and data**

Control how Twitter personalizes content and collects and shares certain data.

Personalization and data

This will enable or disable all of the settings on this page.

11. Finally, identify the "Twitter for teams" section. It is important to stay in control of who has access to your profile. We recommend you turn the "Twitter for teams" switch off. This will make it so no one can add you to a team without your permission.

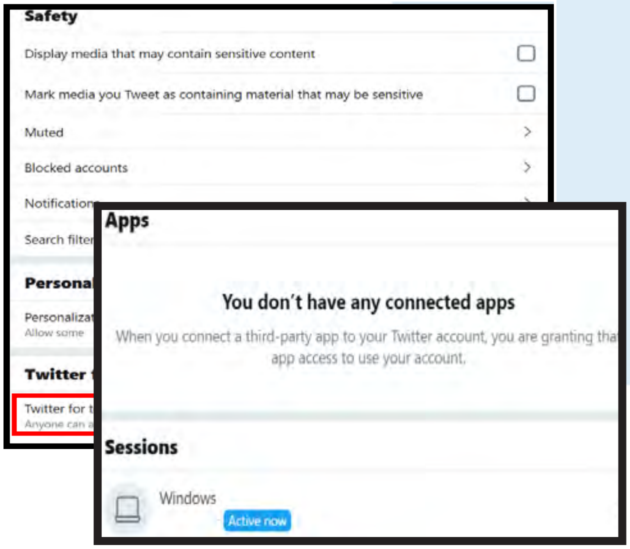


← **Twitter for teams**

Twitter for teams

Organizations can invite anyone to Tweet from their account using the teams feature in TweetDeck
Learn more

12. In order to manage your apps and/or sessions go to "Account" and on the right hand column select "Apps and Sessions". Here you can go through any apps you may have granted access to your Twitter account and revoke access. Limit which apps have access to your account and your personal information.



Safety

Display media that may contain sensitive content ☐

Mark media you Tweet as containing material that may be sensitive ☐

Muted >

Blocked accounts >

Notification

Search filter

Persona

Personaliz
Allow some

Twitter f

Twitter for t
Anyone can a

Apps

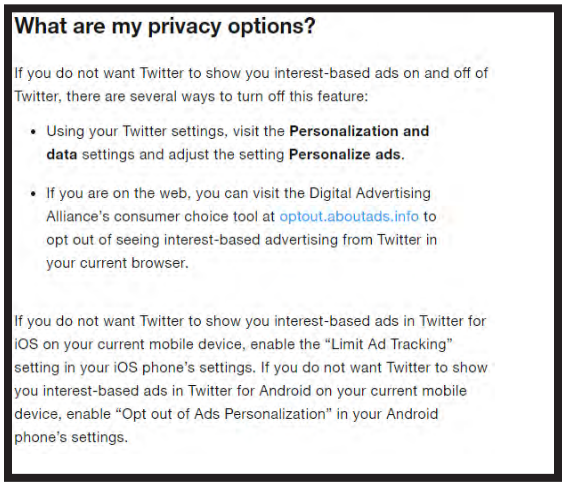
You don't have any connected apps

When you connect a third-party app to your Twitter account, you are granting tha
app access to use your account.

Sessions

Windows
Active now

13. If you prefer to opt out of Twitter's interest-based ads, follow these instructions: go to optout.aboutads.info which will then take you outside of Twitter to the Digital Advertising Alliance page where you can not only opt out of ads from Twitter but other ads that might be using your "cookies" to track you. You do need to be logged into Twitter in order to remove the interest-based ads from your account. Additionally, if you are blocking your cookies, you may have to allow access to them prior to beginning the removal process.



What are my privacy options?

If you do not want Twitter to show you interest-based ads on and off of Twitter, there are several ways to turn off this feature:

- Using your Twitter settings, visit the **Personalization and data** settings and adjust the setting **Personalize ads**.
- If you are on the web, you can visit the Digital Advertising Alliance's consumer choice tool at optout.aboutads.info to opt out of seeing interest-based advertising from Twitter in your current browser.

If you do not want Twitter to show you interest-based ads in Twitter for iOS on your current mobile device, enable the "Limit Ad Tracking" setting in your iOS phone's settings. If you do not want Twitter to show you interest-based ads in Twitter for Android on your current mobile device, enable "Opt out of Ads Personalization" in your Android phone's settings.

App Permissions: Third-party apps may request access to perform different actions using your Twitter account. Apps with "read access" can view your profile info, Tweets, and account settings. Apps with "read and write" access can view the above information, as wells as update and manage your profile and account settings, and post, delete, and engage Tweets on your behalf. Always keep an eye on your "Connected Apps", especially what permissions they have.

Mobile Device Version

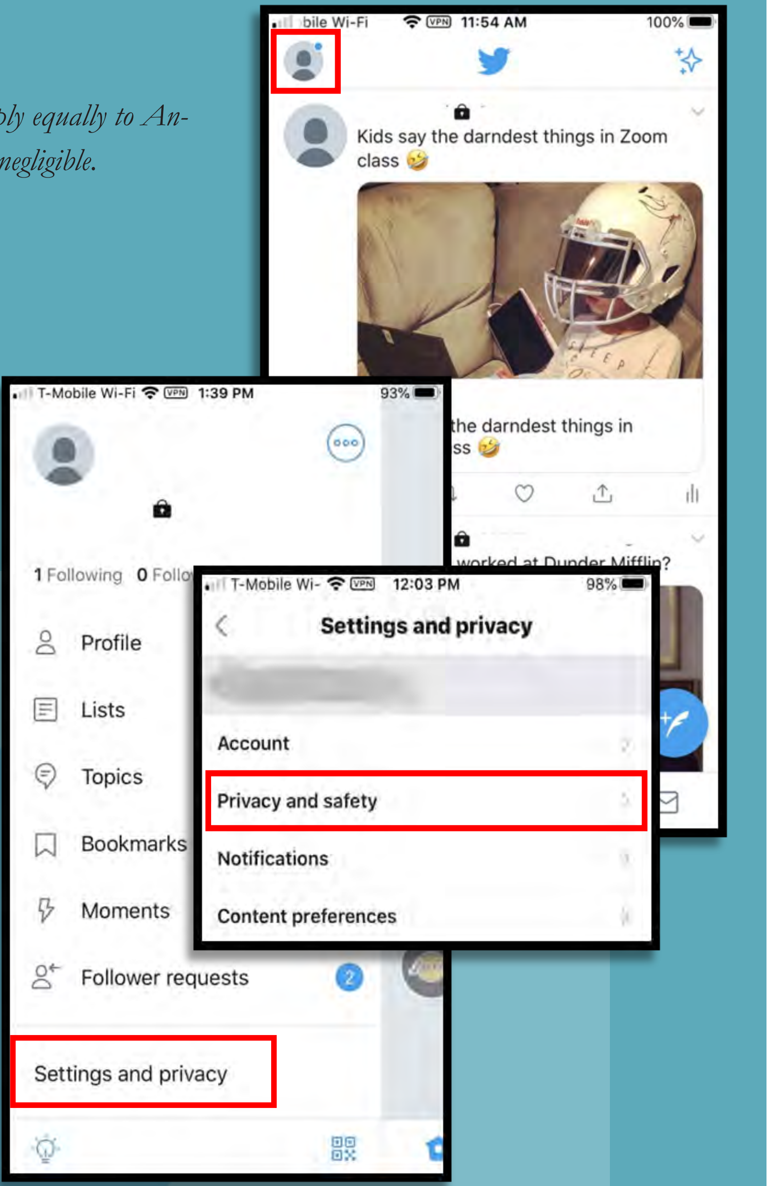
** Images are of iPhone Operating System (iOS), but the steps apply equally to Android Operating System (aOS), as differences between the two are negligible.*

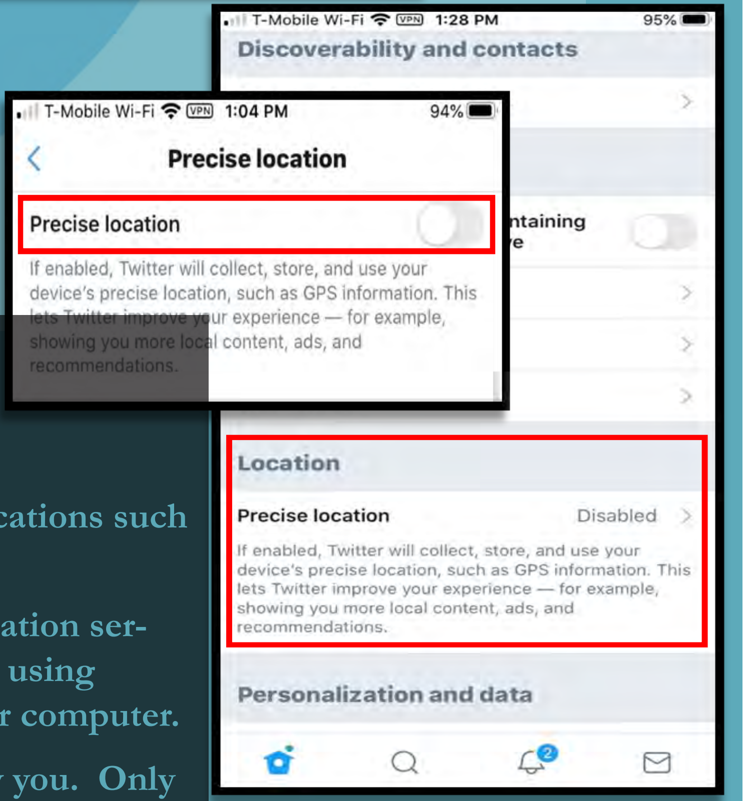
If you frequently access Twitter on your mobile device, you will want to ensure all of the above procedures are completed. Additionally, you will want to accomplish one lockdown feature that is ONLY available on your smart device—the "Precise Location" feature. It is important to turn this feature off because it allows Twitter access to your location for advertisements and photo geo-tagging.

Getting to the "Settings" section on your smart phone is one of the biggest differences between the computer-based and phone-based accounts and is shown in the screenshots displayed on this page.

IPhone users: select the "Profile" icon at the top left of the screen, then select "Settings and Privacy" at the bottom of the menu. Next, select "Privacy and Safety", scroll all the way down to "Location", and "Precise Location" to ensure it is disabled. (see images)

Android users: getting to the "Settings and Privacy" section is similar to the computer based version. Once you are in the "Settings and Privacy" link, select "Privacy and Safety" then scroll down to the bottom of the page and select "Precise Location." We recommend that you turn this function to "disable" and then select "done." (images not provided, but similar)




T-Mobile Wi-Fi 1:28 PM 95%
Discoverability and contacts
ntaining
e
T-Mobile Wi-Fi 1:04 PM 94%
Precise location
Location
Personalization and data

Precise location

If enabled, Twitter will collect, store, and use your device's precise location, such as GPS information. This lets Twitter improve your experience — for example, showing you more local content, ads, and recommendations.

Precise location Disabled

If enabled, Twitter will collect, store, and use your device's precise location, such as GPS information. This lets Twitter improve your experience — for example, showing you more local content, ads, and recommendations.

Don't **provide any identifiable information (e.g. name, hobbies, job title, etc.) on your profile or in your Tweets.**

Don't **link your Twitter account to any third party applications such as Facebook, LinkedIn, or fitness apps.**

Don't **allow Twitter to access your location. Disable location services when posting images on whichever device you are using whether it be iOS, Android or uploading them from your computer.**

Don't **allow people you do not know in real life to follow you. Only maintain connections with people and pages you know and trust.**

TWITTER SMARTCARD

Have you noticed any of the following:

- Unexpected Tweets posted by your account
- Direct Messages sent from your account that you did not initiate
- Other account behaviors you didn't perform or approve (like following, unfollowing, blocking, etc.)
- A notification from Twitter stating that your account may be compromised
- A notification from Twitter stating that your account information (bio, name, etc.) has changed
- Your password is no longer working or you are being prompted to reset it. *If this occurs it is highly recommended that you sign-in online and change your password immediately.

If you said "Yes" to any of the above , Twitter advises you take the following actions:

- Delete any unwanted Tweets that were posted while your account was compromised
- Scan your computers for viruses and malware, especially if unauthorized account behaviors continue to be posted after you've changed your password
- Make sure to change your password. Always use a strong password you haven't used elsewhere and would be difficult to guess
- Consider using login verification (if you haven't done so already), instead of relying on just a password. Login verification introduces a second check to make sure that you and only you can access your Twitter account
- Be sure to check that your email is secure. It may be worth changing the password to both your Twitter account and the email associated with your Twitter account.

If you need to report Spam/Fake Accounts/Harassment: Go to https://help.twitter.com/en/contact-us
If your account was hacked: https://help.twitter.com/en/safety-and-security/twitter-account-hacked

If you find that your account has been hacked, it is best to let Twitter know by filling out the "Hacked Account" form located on the forms site at: https://help.twitter.com/forms

If you cannot log in to your email account, Twitter has provided links to each email accounts "having trouble signing in" page for your convenience. https://help.twitter.com/en/managing-your-account/cant-access-my-accounts-email-address

If you still need help or have questions, you can contact
Twitter using their Support handle @TwitterSupport.

Important Message from Twitter: Changing an account's password does not automatically log the account out of Twitter for iOS or Twitter for Android applications. In order to log the account out of these apps, sign in online and visit "Apps" in your settings. From there you can revoke access for the application, and the next time the app is launched, a prompt will request that the new password be entered. If you frequently receive password reset messages that you did not request, you can require that your email address and/or phone number must be entered in order to initiate a password reset. Find instructions and information about resetting your password.

INSTAGRAM SMARTCARD

MOBILE DEVICE VERSION

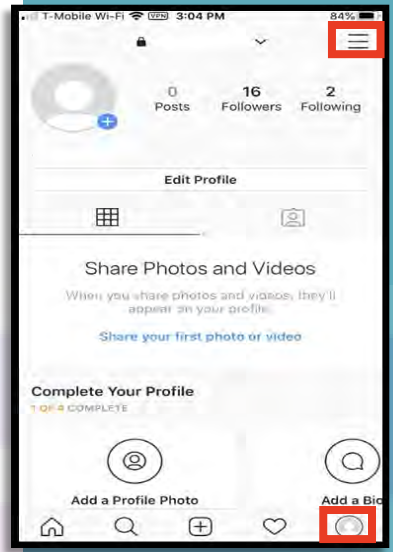
*** Images are of iPhone Operating System (iOS), but the steps apply equally to Android Operating System (aOS), as differences between the two are negligible.**

Instagram now provides you with the ability to update your settings on either your mobile device or computer! It is important to note that some settings are available only on your smart device and a few are only available on your computer, most of the settings are available on your smart device!

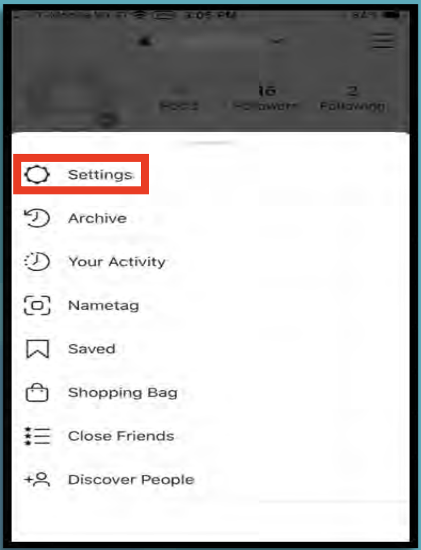
First, it is highly recommended that you set your account to "Private". In the mobile application, head to the bottom of the interface to the "Profile" icon (noted to the right) and select it.

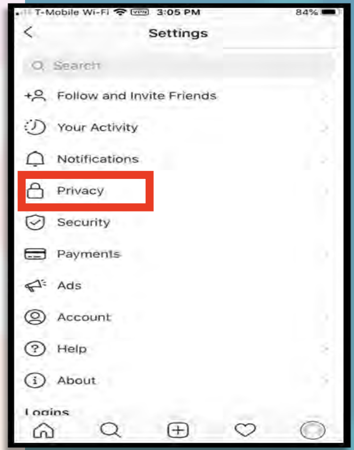
Next, select the "Menu" icon located at the top right of your screen. Select the first option, "Settings", then select "Privacy." (Android: "Settings" located bottom of "Menu" section.)

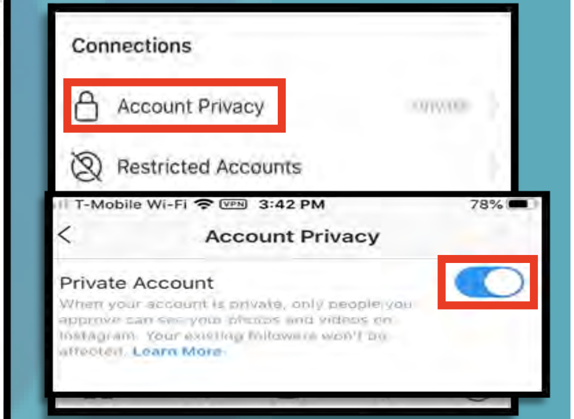
Next, under "Connections", half way down the menu, select "Account Privacy", then turn "On" the "Private Account" toggle. If you are on your computer, the "Settings" icon will be located right next to the "Edit Profile" tab. From there, go back to the "Privacy" tab.



When you share photos and videos, they'll appear on your profile.





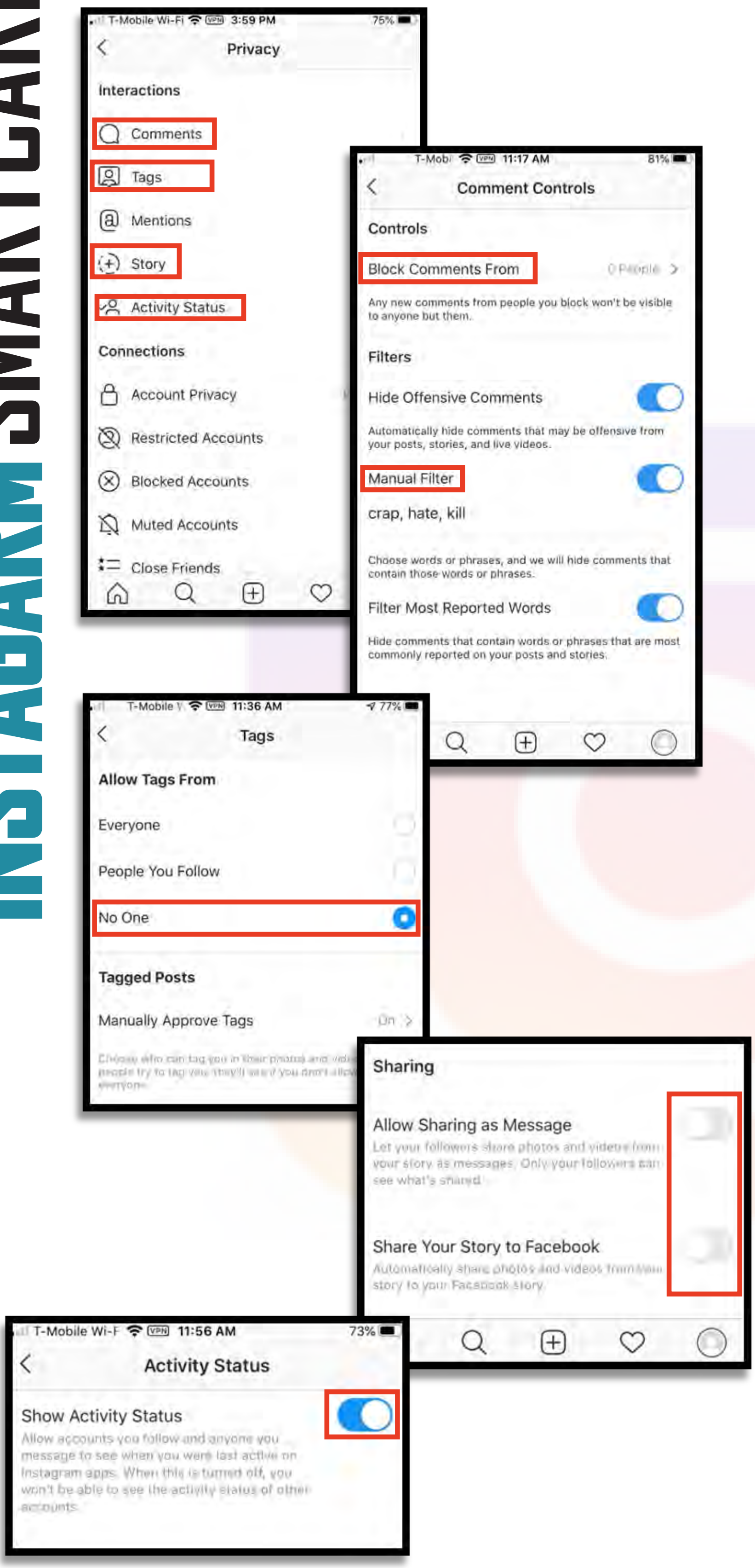


When your account is private, only people you approve can see your photos and videos on Instagram. Your existing followers won't be affected.

- Don't use geo-location tags—this will prevent others from seeing your location. Instagram deletes metadata from a photo the moment of uploading; however, geo-tags that give your location pose a personal security risk.
- Don't establish connections with people you do not know. Understand that people are not always who they say they are online.
- Don't forget to remind family members to take similar precautions with their accounts. Their privacy and share settings can expose your personal data.

- Do use caution when posting images and videos of you or your family. Be aware of your surroundings, to include identifiable locations and any other personal security vulnerabilities.
- Do remember there are privacy concerns when using your name and birthdate when registering for free services, such as apps and social media. It is not necessary to use your real name or birthdate when creating an account.
- Do change your password periodically and turn on Two-Factor Authentication to help keep your account secure.

INSTAGARM SMARTCARD



T-Mobile Wi-Fi 3:59 PM 75%

Privacy

Interactions

- Comments
- Tags
- Mentions
- Story
- Activity Status

Connections

- Account Privacy
- Restricted Accounts
- Blocked Accounts
- Muted Accounts
- Close Friends

T-Mobi 11:17 AM 81%

Comment Controls

Controls

Block Comments From — 0 People >

Any new comments from people you block won't be visible to anyone but them.

Filters

Hide Offensive Comments — On

Automatically hide comments that may be offensive from your posts, stories, and live videos.

Manual Filter — On

crap, hate, kill

Choose words or phrases, and we will hide comments that contain those words or phrases.

Filter Most Reported Words — On

Hide comments that contain words or phrases that are most commonly reported on your posts and stories.

T-Mobile 11:36 AM 77%

Tags

Allow Tags From

- ○ Everyone
- ○ People You Follow
- ● No One

Tagged Posts

Manually Approve Tags — On >

Choose who can tag you in their photos and vid… people try to tag you, they'll see if you don't allo… everyone.

Sharing

Allow Sharing as Message — Off

Let your followers share photos and videos from your story as messages. Only your followers can see what's shared.

Share Your Story to Facebook — Off

Automatically share photos and videos from your story to your Facebook story.

T-Mobile Wi-F 11:56 AM 73%

Activity Status

Show Activity Status — On

Allow accounts you follow and anyone you message to see when you were last active on Instagram apps. When this is turned off, you won't be able to see the activity status of other accounts.

There are many useful features under the "Privacy" tab. First under "Privacy", choose "Comments", then adjust the settings under "Controls". Especially for children's/teen's Instagram accounts, you may want to filter the kinds of feedback allowed on their posts. Here, you can block comments from certain people, and filter out offensive comments including specific words you designate yourself. (see left)

Next, you want to make sure you are in full control of pictures of you that are online - for this, review the "Tags" menu. From the "Privacy" menu, select "Tags". For best security, identify "Allow Tags From" and select "No One", which will allow no one to tag you in their photos. Alternatively, choose "People You Follow". Also, under "Tagged Posts", ensure that "Manually Approve Tags" is noted "On", or select this option and toggle it "On". (see left)

In "Privacy" you will also see "Activity Status". This function allows users to see when you are active on Instagram. If you do not want users to know when you are active you can select "Activity Status" and then toggle "On" to "Off."

Android users: Under "Account Data", you can view all changes to your account—use this feature as an activity feed to ensure actions taken on your account have been your own.

Next, head to "Story" listed under "Privacy" (see left). Identify the section titled "Sharing", toward the bottom of the page. Here you will be able to turn off the "Allow Sharing as Message" function, which allows others to share stories that you have posted. It is also recommended that you take a second to ensure the "Share Your Story to Facebook" function is "Off".

It is also recommended that all settings are reviewed in this section and the setting for "Allow Resharing to Stories" be turned "Off" as well.

80% of Instagram users are from outside of the US. Therefore it is extremely important to vet your followers before you trust them with your profile. #trustbutverfiy

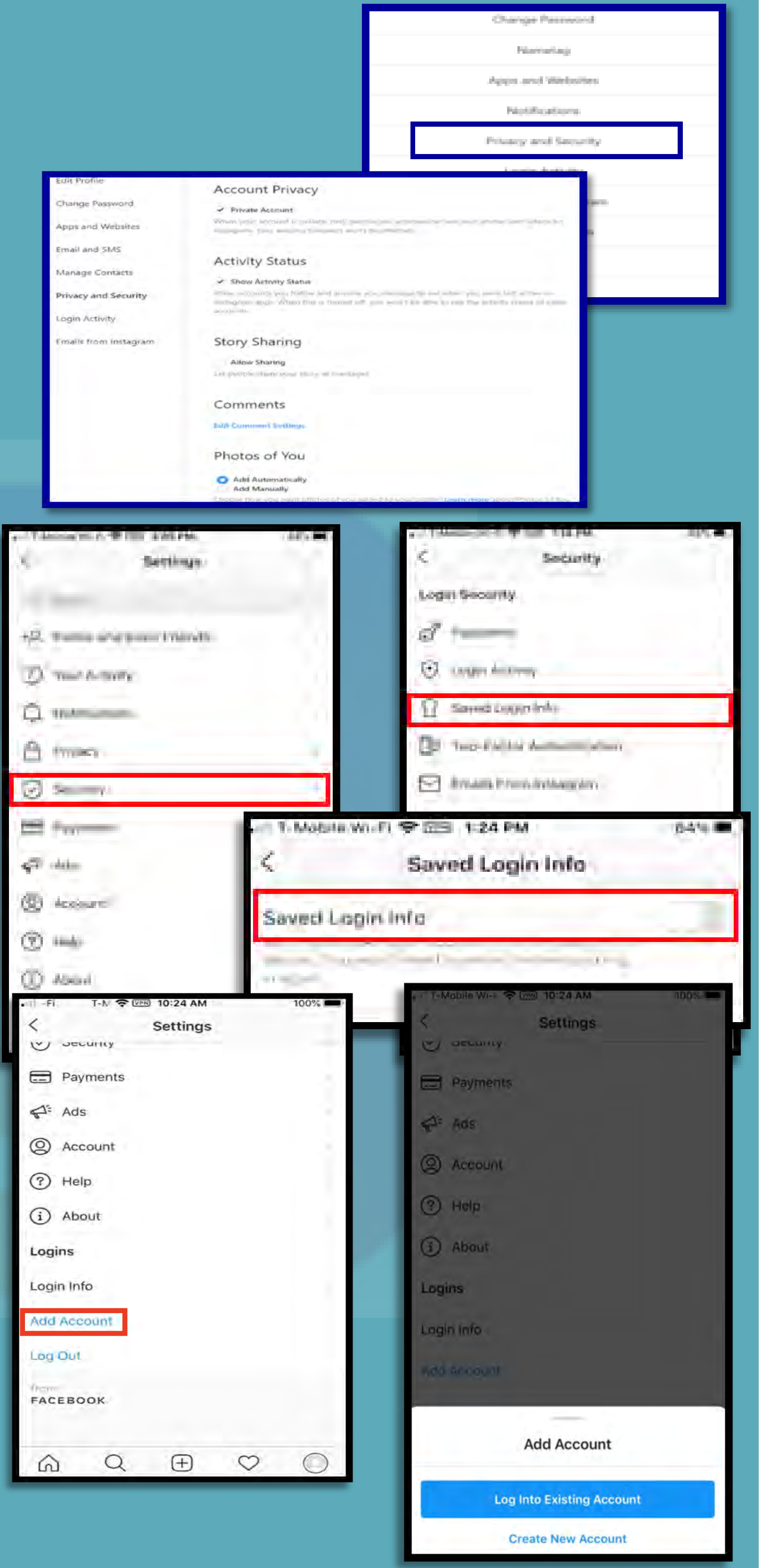
INSTAGRAM SMARTCARD

The remaining items under the "Privacy" tab allow you to restrict, block, and mute Instagram accounts as you see fit. Once you have adjusted the "Privacy" settings on your mobile device, it is a good idea to check them on your computer application as well, to ensure your preferences have been updated. To get to "Settings", from the "Home Page", select your profile icon to the right of your screen, then select the "Settings" icon from the drop down menu that appears or you can select "Profile" then "Edit Profile". (see boxes to the right in blue for computer application.)

With your "Privacy" secured, the next important feature to address is "Security" on your Instagram account. Back under "Settings", select "Security", right under the "Privacy" section you just completed. First, select "Saved Login Info", then ensure the toggle is set to "Off". This way, if someone steals your phone, they will not also have instant access to your Instagram account.

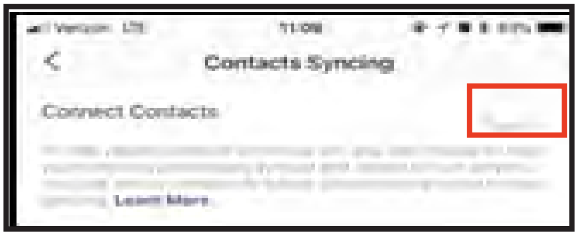
"Next, under "Security", select "Two-Factor Authentication." It is recommended that you choose this function in order to better protect your account. On the following screen, select "Get Started", then choose your preferred authentication method, probably "Text Message".

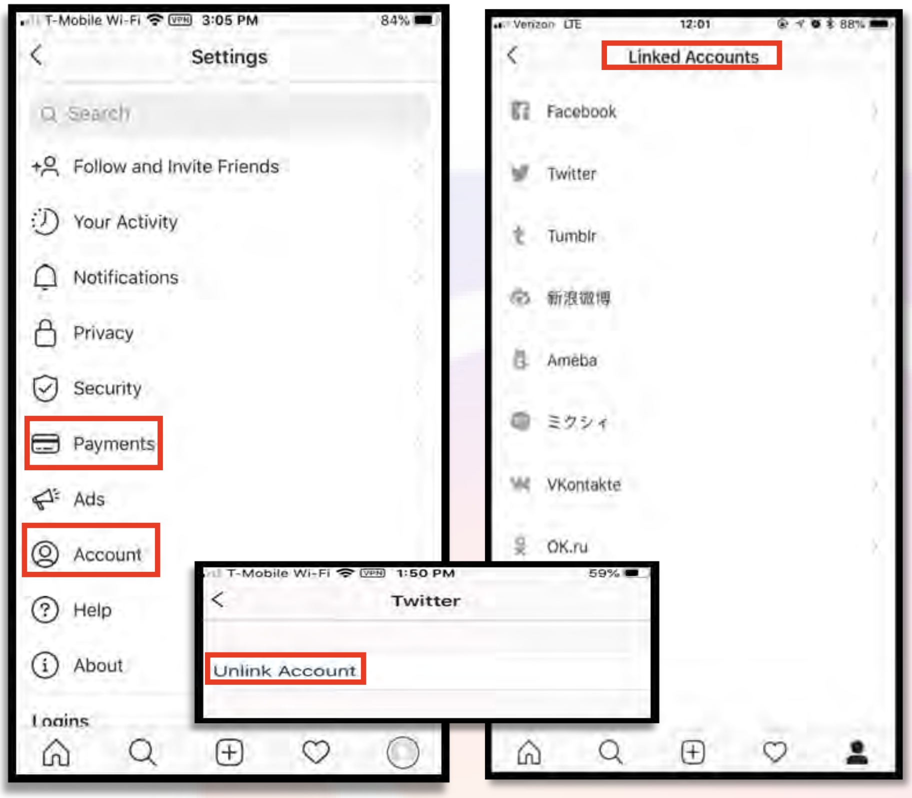
There is a function located in "Settings", called "Add Account", by which you can add unlimited additional accounts to your mobile device. For instance, a parent would be able to add the child's account



The dangers of the "Add Account" feature is significant for teenagers, who are not inclined to consider security and worse case scenarios. No one should allow others to "Add Account". In fact, you should try not to access your account on someone else's mobile device, and always remember to log out, especially when using a different device. Dangers of this situation include: friends can post on your behalf, on your account; friends can send messages on your behalf; friends can do all these things when they become angry with you. The dangers are obvious when considering common teenage behavior.

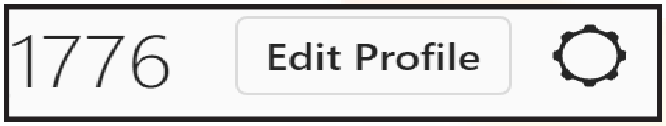
INSTAGARM SMARTCARD

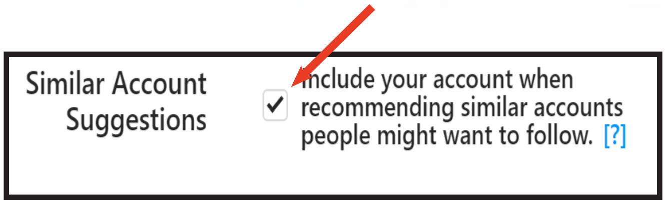




to theirs here, and monitor activity. Depending on the settings of the account, you may be able to access the added account without entering a password. Next, head back to the “Settings” menu and select “Account” then “Contacts Syncing”. It is recommended that you forbid Instagram from uploading your contacts by turning “Off” the “Connect Contacts” option.

Finally, for Android Users, back under “Settings”, notice the option for “Payments”. (see left) This feature allows you to add a “Payment Method” to your Instagram account. It is not advisable to store credit card or any other payment information on your account.
Next, let’s go back to the “Account” menu (under “Settings”) and scroll down to the “Linked Accounts” tab. Here you want to make sure you have not linked any of your social media accounts to Instagram. If you have, you will see the username of the particular account to the left of the arrow. The example (left) is clear of connections. If you have any accounts linked, simply select the arrow next to the social media app and unlink the account by selecting “Unlink Account”. Please do check this, even if you believe you have never manually linked an account, just to make sure.



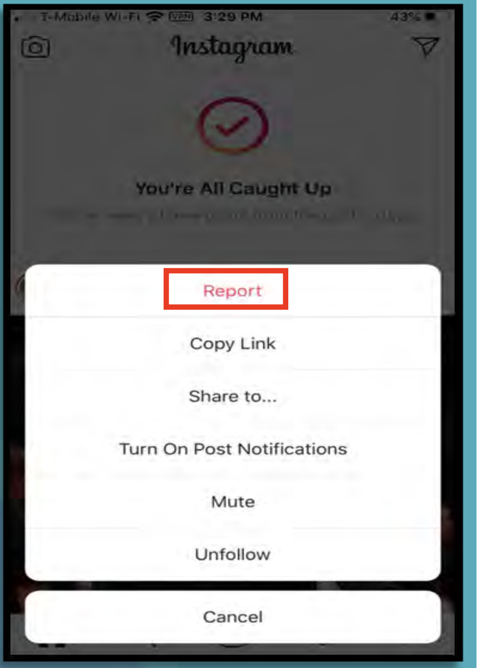


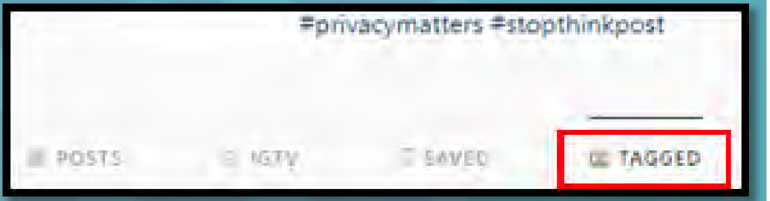
Similar Account Suggestions ☑ Include your account when recommending similar accounts people might want to follow. [?]

Instagram (on your personal computer / laptop) has a feature that allows it to push your profile to other users as “suggested users to follow”, it is recommended you disable this feature. First, select the “Profile” icon, then select the “Edit Profile” button. Once there, scroll to the bottom of the page

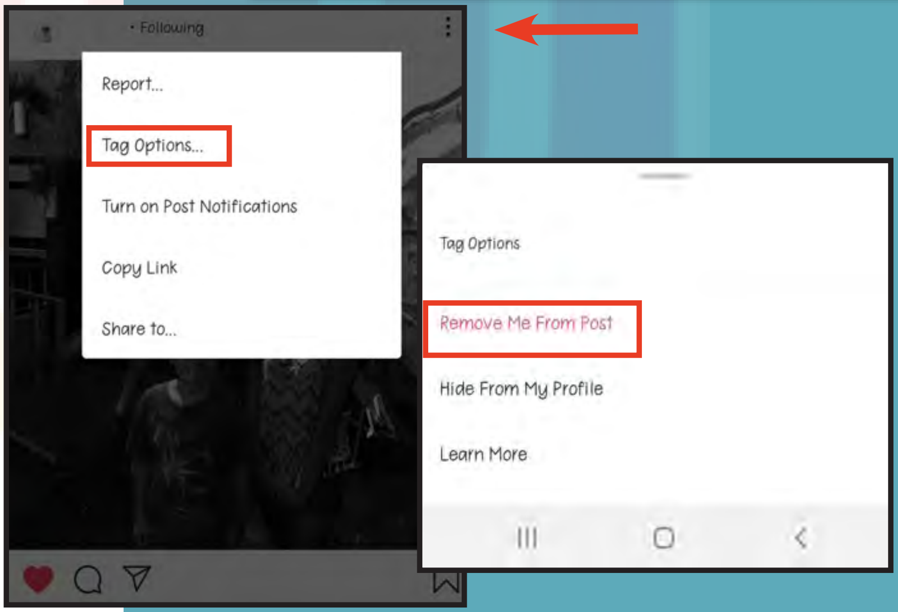
Teenagers use Instagram more so than any other social networking site. It is important to know who they follow, who they allow to follow them and what they are reading and posting. #keepthemsafe and find "Similar Account Suggestions" and deselect the box if checked. Once deselected, Instagram will no longer be allowed to push your profile to other users as "suggested users to follow." *This feature can only be locked down on your computer application.

Instagram allows you to report, or remove from your feed, any offensive post you come across. Simply select the menu button at the top right corner of the post and select which option best applies to that particular post from the drop-down menu. You have options to "Report" the offensive post, "Mute" the account that posted it for a select period of time, or "Unfollow" the person who posted it. When you report a post, Instagram will ask you for more information as to why you are reporting it, and then offer suggestions to improve your Instagram experience.





Removing unwanted tagged photos/posts is important. If you have a profile that is "Private," you are on the right track to controlling your online image. Understand that even if your profile is private, if you tag or comment on a post from a public profile, your tag or comment will be viewable to all.



In order to remove a tag of yourself from someone else's post you can follow these steps. First, go back to your "Profile" icon and select the "Tagged" icon (see right). Next, select the post you are tagged in that you wish to un-tag yourself from. Find and select the menu at the bottom of the post (shown to the left of the page by a red box), then select "Tag Options." Next, you can "Remove Me From Post" simply by selecting the link highlighted here in red. *This may not be available on all devices, such as iPhone, but it is available on computer.

Instagram allows you to have more than one account loaded at a time. Talk to your kids about sharing their usernames and passwords with their friends. #protectourkids

INSTAGRAM SMARTCARD

HACKED

Have you noticed any of the following:

- Unexpected posts posted by your account
- Direct Messages sent from your account that you did not initiate
- Other account behaviors you didn't perform or approve (like following, unfollowing, blocking, etc.)
- A notification from Instagram stating that your account may be compromised
- A notification from Instagram stating that your account information (bio, name, etc.) has changed
- Your password is no longer working or you are being prompted to reset it. *If this occurs it is highly recommended that you sign-in online and change your password immediately.

If you said "Yes" to any of the above , it is advised you take the following actions:

- Delete any unwanted posts that were posted while your account was compromised
- Scan your computers for viruses and malware, especially if unauthorized account behaviors continue to be posted after you've changed your password
- Make sure to change your password. Always use a strong password you haven't used elsewhere and would be difficult to guess
- Consider using login verification (if you haven't done so already), instead of relying on just a password. Login verification introduces a second check to make sure that you and only you can access your Instagram account
- Be sure to check that your email is secure. It may be worth changing the password to both your Instagram account and the email associated with your Instagram account. *If you feel your email may have been compromised and need help finding the right contact information for your email provider please see page 21 of this smart book under the "blue box" at the bottom of the page.

If you need to report Spam/Harassment: Go to https://help.instagram.com/contact/383679321740945?helpref=page_content

If your account was hacked: https://help.instagram.com/, then go to "Privacy and Safety Center," "Report Something," and finally select "Hacked."

Also, if you find that someone is impersonating you on Instagram: Go to https://help.instagram.com/, then go to "Privacy and Safety Center", "Report Something," and finally select "Impersonation Accounts."

If you still need help or have questions, you can always contact Instagram by: https://help.instagram.com/contact/272476913194545?helpref=faq_content

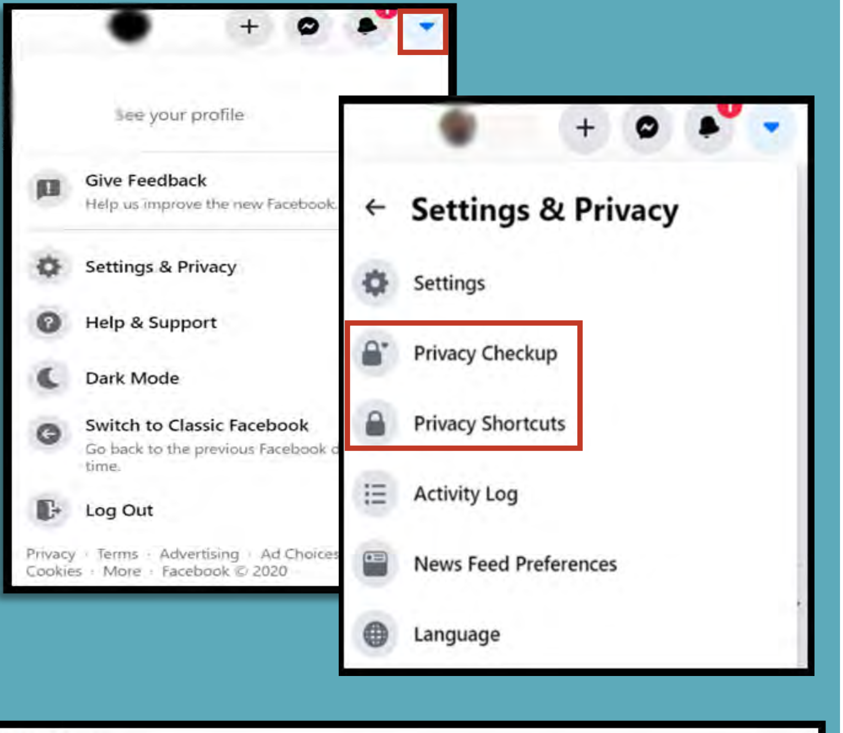
If you received an email from Instagram letting you know that your email address was changed, you may be able to undo this by using the revert this change option in that message. If additional information was also changed (example: your password), and you're unable to change back your email address, then you should report the account to Instagram.

PERSONAL COMPUTER (PC) VERSION

New Design & Quick Privacy

Facebook published a new platform design in 2020, with the purposes of providing a simplified user experience closer to the mobile app version, faster performance, and new features. Facebook's new design provides several privacy and security updates, most notably more access to information and explanations regarding your options.

The information provided in these pages will walk through the entire process of locking down your Facebook account. However, if you are in a hurry, you can access an abbreviated version of Facebook's privacy and security options by going through the "Privacy Checkup" and "Privacy Settings" features on your account and then go back to the full version when you are able.



See your profile

Give Feedback
Help us improve the new Facebook

Settings & Privacy

Help & Support

Dark Mode

Switch to Classic Facebook
Go back to the previous Facebook d time.

Log Out

Privacy · Terms · Advertising · Ad Choices
Cookies · More · Facebook © 2020

← Settings & Privacy

Settings

Privacy Checkup

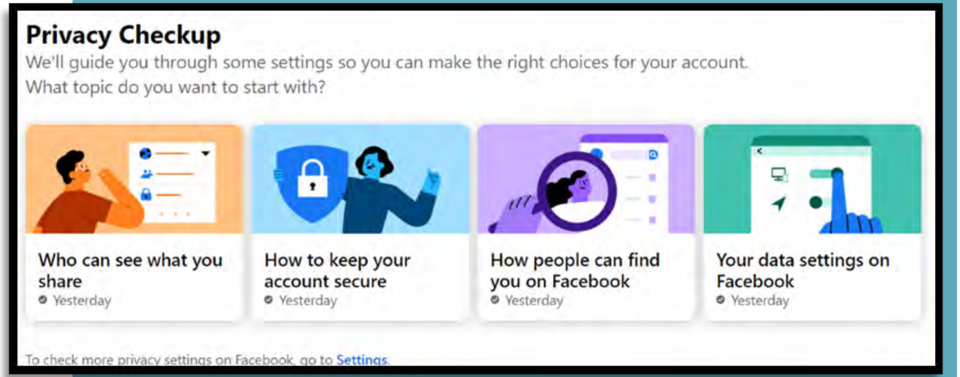
Privacy Shortcuts

Activity Log

News Feed Preferences

Language

Starting at your "Home Page", select the "Down Arrow" in the top right corner (shown here in the top right of the page), select "Settings & Privacy from the drop down. Next, select "Privacy Checkup", and walk through each box on the screen that follows. Again, this is an abbreviated version of the manual provided here, we recommend you work though this whole Card at your convenience.



Privacy Checkup

We'll guide you through some settings so you can make the right choices for your account.
What topic do you want to start with?

Who can see what you share
Yesterday

How to keep your account secure
Yesterday

How people can find you on Facebook
Yesterday

Your data settings on Facebook
Yesterday

To check more privacy settings on Facebook, go to Settings.

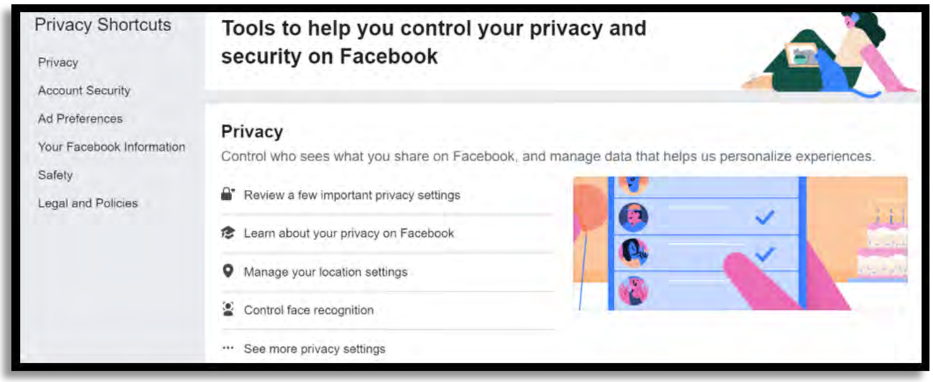
You could also use this feature to complete easy quick checks on a regular basis, for instance each month, just to make sure you stay on top of changes.

Secondly, you can select "Privacy Shortcuts" (shown on the top right of this page), which will take you to the page seen here to the right. Here, you can go through some additional privacy information (all of which will be covered in the coming pages), and access useful information about things like privacy, how Face-

- Do use pictures of something other than yourself for cover and profile photos. Cover and profile photos are viewable to the "Public". Remember if you change your profile picture you must change the privacy setting from "Public" to perhaps "Friends", Facebook will not do it for you.
- Do use caution when posting images and videos of you or your family. Be aware of your surroundings, to include identifiable locations and any other personal security vulnerabilities.
- Do select "Only Me" or "Friends" for all available settings options. Ensure that family members take similar precautions with their accounts. Their privacy and share settings can expose your personal data.

- Don't add your birthdate, location, phone number, or other personal details to your profile. If you do add this information make sure you set it so that it is not "Public".
- Don't link your Facebook account to any third party applications such as Twitter, LinkedIn, or gaming apps.
- Don't establish connections with individuals you do not know and trust. Understand that not everyone is who they say they are.
- Don't discuss specific details online, keep discussions general. When posting pictures, ensure that no personal information can be seen in the background. For instance, if you are posting a picture of your car you will want to make sure the license plate is not showing.

PERSONAL COMPUTER (PC) VERSION



Privacy Shortcuts

Privacy

Account Security

Ad Preferences

Your Facebook Information

Safety

Legal and Policies

Tools to help you control your privacy and security on Facebook

Privacy

Control who sees what you share on Facebook, and manage data that helps us personalize experiences.

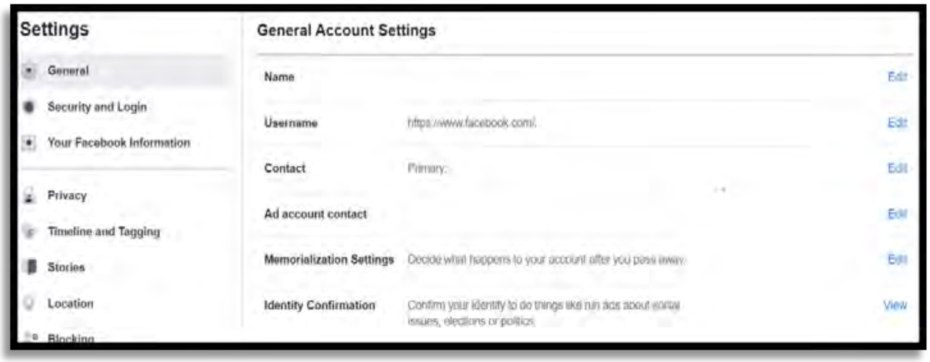
Review a few important privacy settings

Learn about your privacy on Facebook

Manage your location settings

Control face recognition

··· See more privacy settings



Settings

General

Security and Login

Your Facebook Information

Privacy

Timeline and Tagging

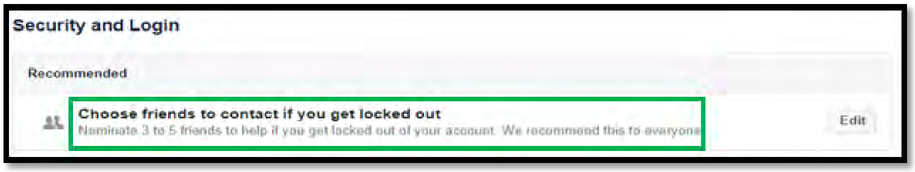
Stories

Location

Blocking

General Account Settings

Name		Edit
Username	https://www.facebook.com/	Edit
Contact	Primary:	Edit
Ad account contact		Edit
Memorialization Settings	Decide what happens to your account after you pass away.	Edit
Identity Confirmation	Confirm your identity to do things like run ads about social issues, elections or politics	View



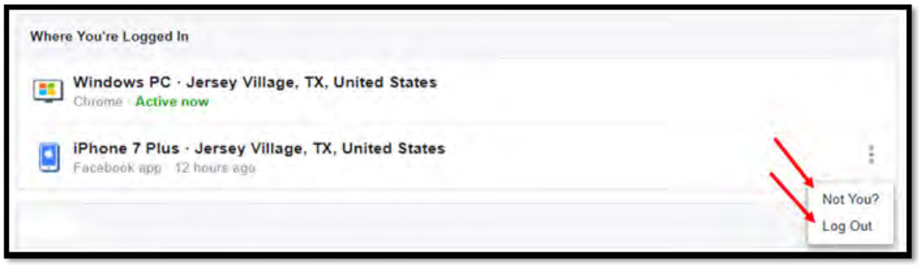
Security and Login

Recommended

Choose friends to contact if you get locked out

Nominate 3 to 5 friends to help if you get locked out of your account. We recommend this to everyone

Edit



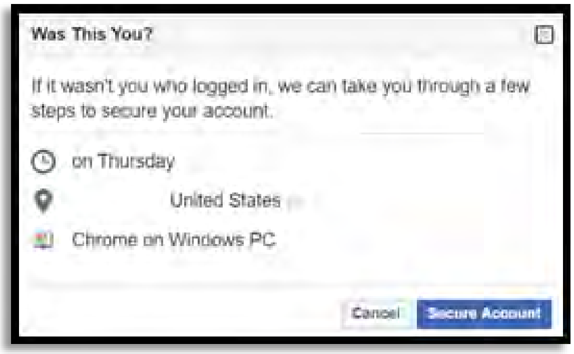
Where You're Logged In

Windows PC · Jersey Village, TX, United States
Chrome · Active now

iPhone 7 Plus · Jersey Village, TX, United States
Facebook app · 12 hours ago

Not You?

Log Out



Was This You?

If it wasn't you who logged in, we can take you through a few steps to secure your account.

on Thursday

United States

Chrome on Windows PC

Cancel | Secure Account

book's ad policy and processes work, and resources for parents. Again, feel free to go through this information, but also complete the full Card, beginning below, for our most thorough lock down guidance.

Facebook continuously works to enhance its privacy efforts and better protect user data. As a result, many settings have changed and more have been added. To begin, click the "Down Arrow" at the top right corner of the Facebook screen. From the drop down, select "Settings and Privacy", then "Settings". You will want to go through each menu item on the next few pages in order to secure your Facebook account.

Starting in the "General" section, go through and review your information. Remember, your "Username" (which will be in the URL) will be "Public" on Facebook, just as your "Name" is. In this section you can add a new email address and phone number, direct what happens with your account when you die, and direct Facebook ads to a new email address.

Head back to the left-hand column and select "Security and Login". Here you can check and up-date your security settings and see where Facebook has you logged in at, to check for discrepancies.

First, look at the "Where You're Logged in at" section and ensure you recognize each location Facebook has you logged in from. Some of these locations can be repetitive based on how many times you log in or for each different session. If you do not recognize a location, you can select the "Not You?" tab, and then the "Secure Account" button. Facebook will take you through steps to help you ensure your account is secure. Next, under "Login", select "Save your login info", you have the choice to keep yourself logged in on any device you choose. We recommend that you NOT enable this function, and instead choose to log in each time you open Facebook. This way your ac-

I think it is important to fortify ourselves online the same way we would fortify our homes if we knew we were under attack.

-II MEF Commanding General LtGen Hedelund's response when asked for his take on social media and force protection.

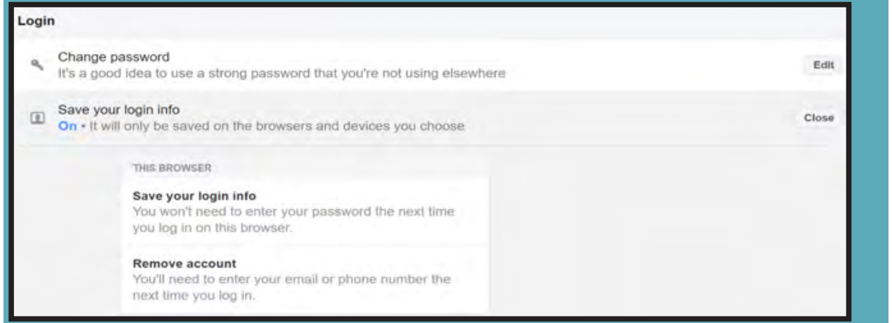
count is secure even if you lose your computer or mobile device. Select the "Edit" button to the right, and then select "Remove saved login info".

We recommend that you enable "Two-factor Authentication" in order to equip your account with the highest level of security available. Click on the "Edit" button to the right of "Use two-factor authentication" and choose the security method you prefer or are most familiar with. A security code will be sent to you for entry each time you log in.

In "Settings Up Extra Security" it is recommended that you choose friends that can help you log in to Facebook should you ever become locked out. This will be especially helpful should your Facebook account get hacked.

It is also a good idea to request notifications in the event that someone logs into your account without your permission. To do this, under "Setting Up Extra Security", and "Get alerts about unrecognized logins", to the right, click the "Edit" button. Then select the buttons under "Facebook Notification", "Messenger" and/or "Email" to direct where you would like to receive such messages. To complete, click on the "Save Changes" button.

Next, go back to the column on the left-hand side and select "Your Facebook information". Here you can easily manage the information you have allowed onto Facebook or delete your account entirely. * Time Saver...both the "Access Your Information" and "Activity Log" sections take you to the same "Activity Log" page and allow you to manage your information.



Login

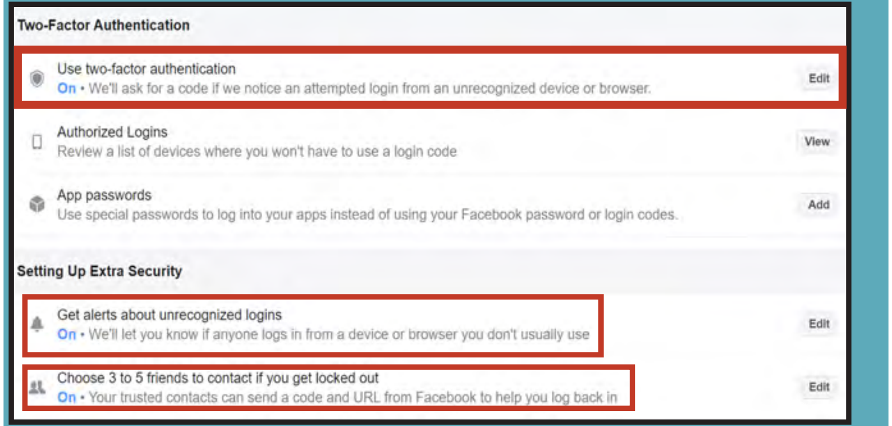
Change password
It's a good idea to use a strong password that you're not using elsewhere

Save your login info
On • It will only be saved on the browsers and devices you choose

THIS BROWSER

Save your login info
You won't need to enter your password the next time you log in on this browser.

Remove account
You'll need to enter your email or phone number the next time you log in.



Two-Factor Authentication

Use two-factor authentication
On • We'll ask for a code if we notice an attempted login from an unrecognized device or browser.

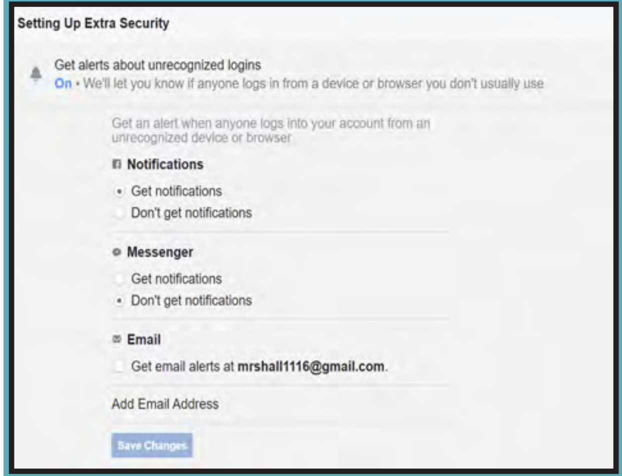
Authorized Logins
Review a list of devices where you won't have to use a login code

App passwords
Use special passwords to log into your apps instead of using your Facebook password or login codes.

Setting Up Extra Security

Get alerts about unrecognized logins
On • We'll let you know if anyone logs in from a device or browser you don't usually use

Choose 3 to 5 friends to contact if you get locked out
On • Your trusted contacts can send a code and URL from Facebook to help you log back in



Setting Up Extra Security

Get alerts about unrecognized logins
On • We'll let you know if anyone logs in from a device or browser you don't usually use

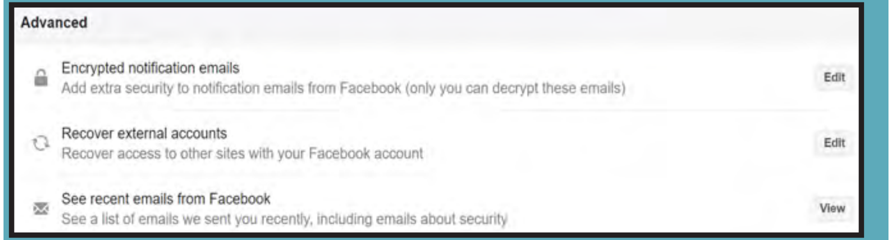
Get an alert when anyone logs into your account from an unrecognized device or browser

Notifications
● Get notifications
○ Don't get notifications

Messenger
○ Get notifications
● Don't get notifications

Email
□ Get email alerts at **mrshall1116@gmail.com**.

Add Email Address



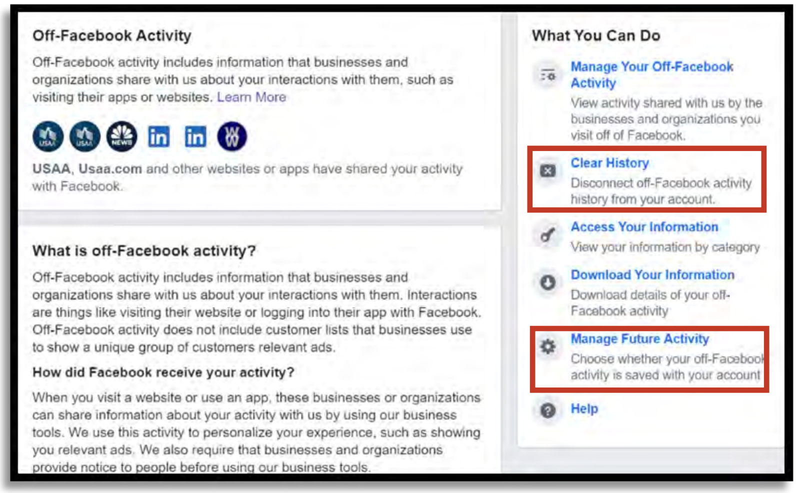
Advanced

Encrypted notification emails
Add extra security to notification emails from Facebook (only you can decrypt these emails)

Recover external accounts
Recover access to other sites with your Facebook account

See recent emails from Facebook
See a list of emails we sent you recently, including emails about security

An unrecognized login location can be the result of a few different things. First, when signing in via mobile device, you may be routed through an IP address that doesn't reflect your actual location. Second, Facebook may have inaccurate information. Third, you may remain logged into a device that you logged onto in an alternate location. And finally someone else could have unauthorized access to your Facebook account. If an unrecognized location seems to be due to unauthorized access it is recommended that you immediately go in and change your password on both Facebook and your email account.



Off-Facebook Activity

Off-Facebook activity includes information that businesses and organizations share with us about your interactions with them, such as visiting their apps or websites. Learn More

USAA, Usaa.com and other websites or apps have shared your activity with Facebook.

What is off-Facebook activity?

Off-Facebook activity includes information that businesses and organizations share with us about your interactions with them. Interactions are things like visiting their website or logging into their app with Facebook. Off-Facebook activity does not include customer lists that businesses use to show a unique group of customers relevant ads.

How did Facebook receive your activity?

When you visit a website or use an app, these businesses or organizations can share information about your activity with us by using our business tools. We use this activity to personalize your experience, such as showing you relevant ads. We also require that businesses and organizations provide notice to people before using our business tools.

What You Can Do

Manage Your Off-Facebook Activity
View activity shared with us by the businesses and organizations you visit off of Facebook.

Clear History
Disconnect off-Facebook activity history from your account.

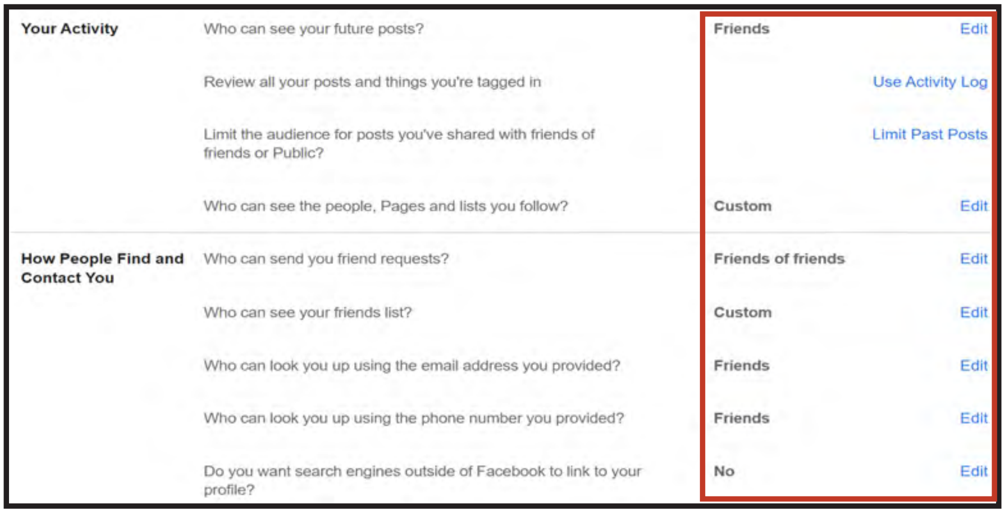
Access Your Information
View your information by category

Download Your Information
Download details of your off-Facebook activity

Manage Future Activity
Choose whether your off-Facebook activity is saved with your account

Help

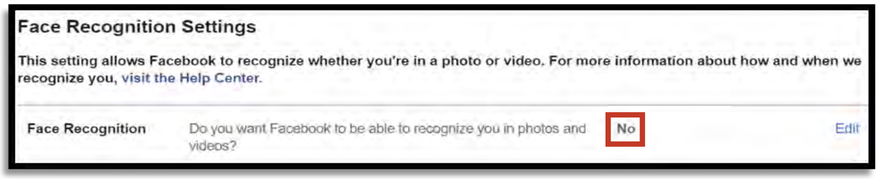
Next select "Off-Facebook Activity" and clear your history. It is highly recommended that you forbid Facebook from tracking your "Off-line Activity. Select "Clear History" and click on the "Clear History" button on the pop-up. Also consider selecting "More Options", then "Manage Future Activity" in order to limit the kinds of information Facebook can collect from your "Off-Facebook Activity" in the future. Follow the prompts to "Manage Future Activity".



Your Activity	Who can see your future posts?	Friends	Edit
	Review all your posts and things you're tagged in		Use Activity Log
	Limit the audience for posts you've shared with friends of friends or Public?		Limit Past Posts
	Who can see the people, Pages and lists you follow?	Custom	Edit
How People Find and Contact You	Who can send you friend requests?	Friends of friends	Edit
	Who can see your friends list?	Custom	Edit
	Who can look you up using the email address you provided?	Friends	Edit
	Who can look you up using the phone number you provided?	Friends	Edit
	Do you want search engines outside of Facebook to link to your profile?	No	Edit

Now head back to your "Settings" page and select "Privacy" from the tabs on the left-hand side. Completing this section is one of the most important aspects to keeping your information safeguarded on Facebook. This section puts you, the user, in charge of decisions about where your data goes and who can see it. Take some time here to ensure each section is set to your preference. It is recommended no category be set to "Public". While it is unrealistic to select "Only Me" to every option here, be sure that each "Friend" you allow access to your information is trustworthy and a known entity. If you have "Friends" on your Facebook that you do not necessarily trust in your inner circle it is a good idea to select "Only Me" where your personal information is concerned (see red block to the left).

We recommend choosing "Only Me" wherever possible but understand that this sometimes undermines the social purpose of Facebook. Still, we strongly recommend you leave the "Only Me" setting for "Who can see your friends list" in order to protect yourself and your social network—this list simply gives away too much information about you. Where you cannot leave "Only Me", the next best option is to choose "Friends". Finally, we recommend you do not allow Facebook to link other search engines to your profile.



Face Recognition Settings

This setting allows Facebook to recognize whether you're in a photo or video. For more information about how and when we recognize you, visit the Help Center.

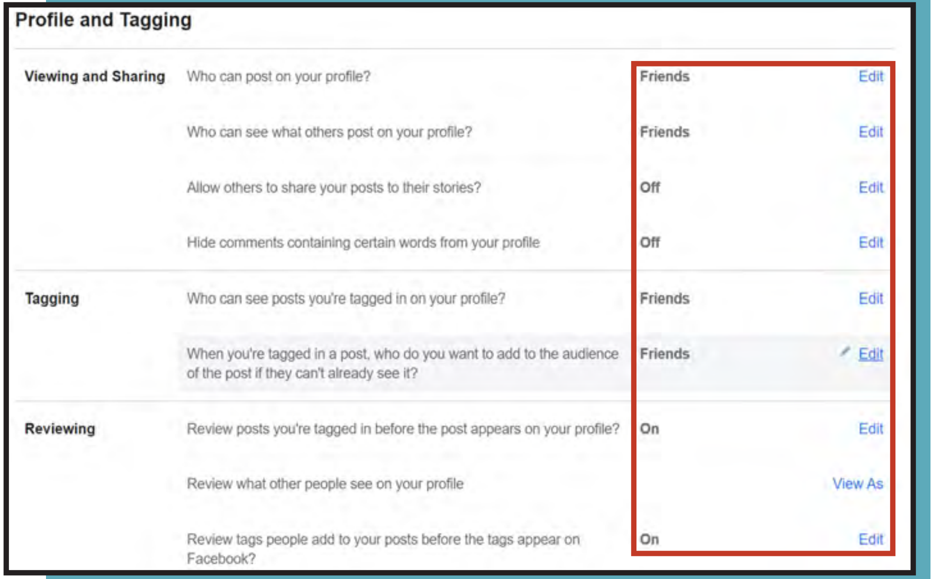
Face Recognition	Do you want Facebook to be able to recognize you in photos and videos?	No	Edit

Next, head back over to the left side "Settings" menu, find and select "Face Recognition". It is recommended here that you not allow Facebook to recognize your face in videos or photos. Simply select "Edit" and from the drop-down menu that appears and then select "No".

Never become complacent with your Privacy settings. Checking your settings once a quarter could help to keep your information safe online.

FACEBOOK SMARTCARD

Now select "Profile and Tagging" from the side "Settings" menu. Take a few moments here to make sure you agree with all the settings. Here it is recommended that all items be updated from "Public" to either "Friends" or "Only Me." Also, make sure to turn "On" each section under "Reviewing" so that any "Tag" created with your name on it is reviewed by you in case you do not agree with the content and want the "Tag" removed.

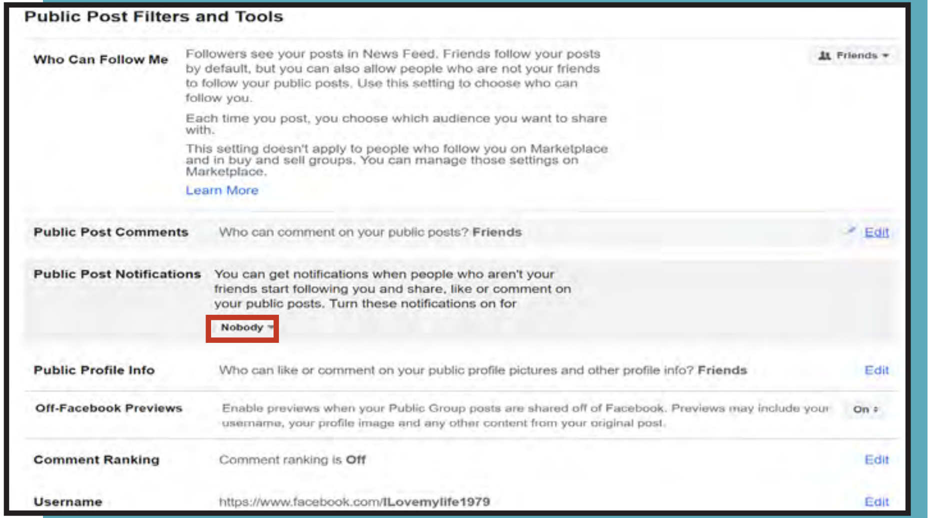


Profile and Tagging

Viewing and Sharing	Who can post on your profile?	Friends	Edit
	Who can see what others post on your profile?	Friends	Edit
	Allow others to share your posts to their stories?	Off	Edit
	Hide comments containing certain words from your profile	Off	Edit
Tagging	Who can see posts you're tagged in on your profile?	Friends	Edit
	When you're tagged in a post, who do you want to add to the audience of the post if they can't already see it?	Friends	Edit
Reviewing	Review posts you're tagged in before the post appears on your profile?	On	Edit
	Review what other people see on your profile		View As
	Review tags people add to your posts before the tags appear on Facebook?	On	Edit

Under "Reviewing", you can also view your profile from the perspective of the public, people who are not your "Friends". Simply select "View As" next to "Review what other people see on your profile". While reviewing your profile from the public perspective, take note of anything you see that you might want to lock down later, such as old profile pictures.

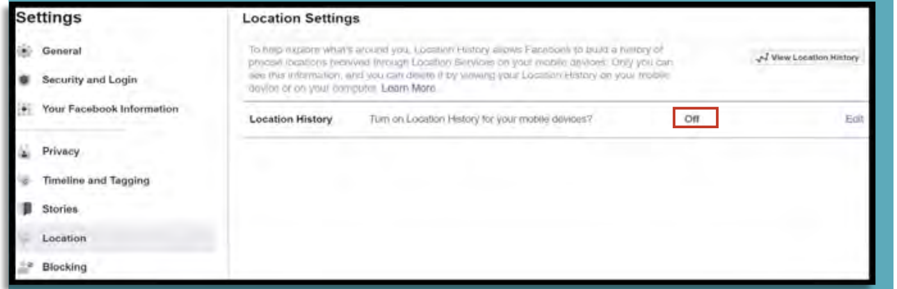
Next, let us review "Public Posts" by selecting it from the left side menu. It is recommended that you not let the "Public" follow you. Remember, allowing the "Public" to follow you means anyone with a Facebook profile, and possibly even without one, can see what you are posting. Here it is also important to review your "Username," this will show up in your Facebook page URL (there is no way to hide it). If you do not want your full name displayed to the Public it is recommended you change your URL, which if not changed will display your full name.



Public Post Filters and Tools

Who Can Follow Me	Followers see your posts in News Feed. Friends follow your posts by default, but you can also allow people who are not your friends to follow your public posts. Use this setting to choose who can follow you. Each time you post, you choose which audience you want to share with. This setting doesn't apply to people who follow you on Marketplace and in buy and sell groups. You can manage those settings on Marketplace. Learn More	Friends
Public Post Comments	Who can comment on your public posts? **Friends**	Edit
Public Post Notifications	You can get notifications when people who aren't your friends start following you and share, like or comment on your public posts. Turn these notifications on for Nobody	
Public Profile Info	Who can like or comment on your public profile pictures and other profile info? **Friends**	Edit
Off-Facebook Previews	Enable previews when your Public Group posts are shared off of Facebook. Previews may include your username, your profile image and any other content from your original post.	On
Comment Ranking	Comment ranking is **Off**	Edit
Username	https://www.facebook.com/**ILovemylife1979**	Edit

In the "Location" section make sure Facebook shows your location as "Off". You must also turn your location settings to "Off" on each of your mobile devices to ensure you do not share location data with Facebook.



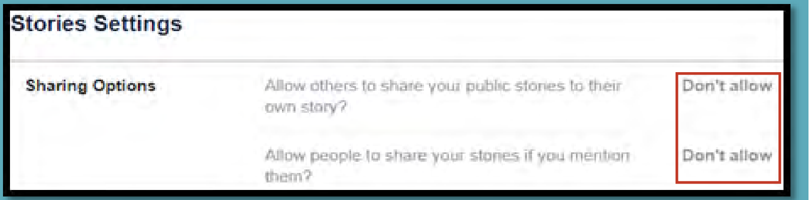
Location Settings

To help explore what's around you, Location History allows Facebook to build a history of precise locations received through Location Services on your mobile devices. Only you can see this information, and you can delete it by viewing your Location History on your mobile device or on your computer. Learn More

View Location History

Location History	Turn on Location History for your mobile devices?	Off	Edit

Since the "Stories" function has become more popular, it is important to remember it also needs to be locked down. Facebook has created a new feature that prohibits others from sharing your "Stories". Select "Stories" from the "Settings" menu and set both "Sharing Options" to "Don't Allow".

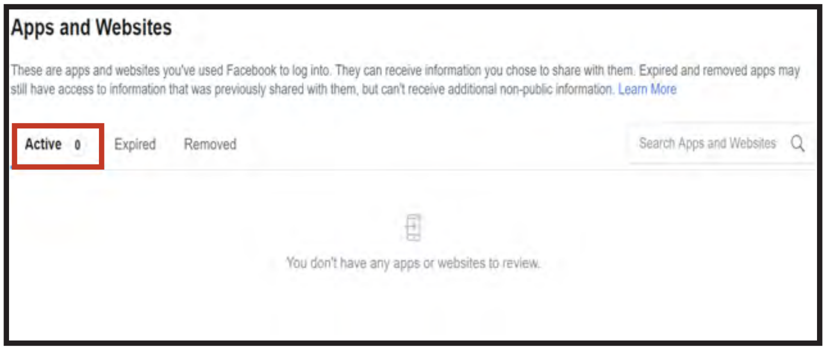


Stories Settings

Sharing Options	Allow others to share your public stories to their own story?	Don't allow
	Allow people to share your stories if you mention them?	Don't allow

Now let's clean up the "Apps and Websites" section on Facebook. For security purposes this section should have zero apps and/or websites listed. If there are any apps or websites listed this means you have allowed either of them to log you in with your Facebook account instead of creating a new account. It is highly

Managing your Facebook Profile is important. Equally as important, is knowing what other users are saying about you. #ownyourprofile #fbtagging



Apps and Websites

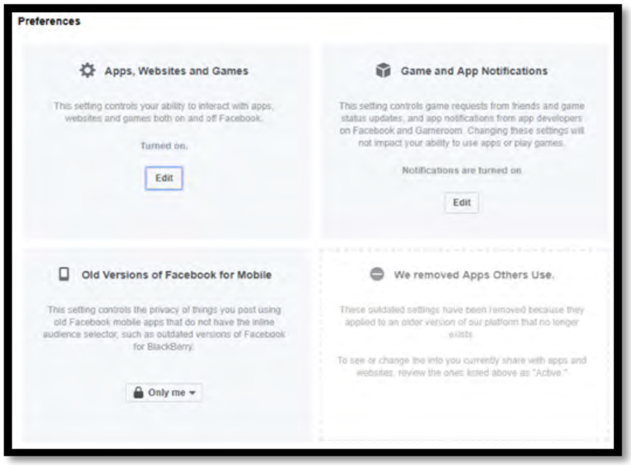
These are apps and websites you've used Facebook to log into. They can receive information you chose to share with them. Expired and removed apps may still have access to information that was previously shared with them, but can't receive additional non-public information. Learn More

You don't have any apps or websites to review.

recommended that you do not allow other apps or websites to log you in with any other social media.

If you have allowed apps or websites access to your Facebook account, you can remove and delete that access here. Make sure to check the "Active" and "Expired" section tabs at the top of this box.

Next scroll down to the "Preferences" section on the same page. Here you can control how "Apps, Websites, and Games" are able to interact with your Facebook account. We recommend that you keep the "Old Version of Facebook for Mobile" in a setting set to "Only Me" so that it is not viewable to anyone else.



Preferences

Apps, Websites and Games

This setting controls your ability to interact with apps, websites and games both on and off Facebook.

Turned on.

Game and App Notifications

This setting controls game requests from friends and game status updates, and app notifications from app developers on Facebook and Gameroom. Changing these settings will not impact your ability to use apps or play games.

Notifications are turned on

Old Versions of Facebook for Mobile

This setting controls the privacy of things you post using old Facebook mobile apps that do not have the inline audience selector, such as outdated versions of Facebook for BlackBerry.

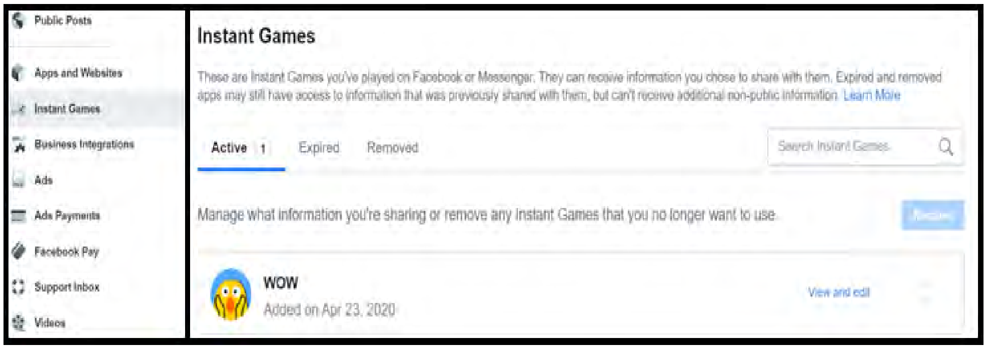
Only me

We removed Apps Others Use.

These outdated settings have been removed because they applied to an older version of our platform that no longer exists.

To see or change the info you currently share with apps and websites, review the ones listed above as "Active."

Now select the "Instant Games" tab in the "Settings" menu. Review any games you may have allowed access to your account, the type of data they are collecting, and whether you want them to remain. If you choose to, you can delete any of the games, much like you just did in the "Apps and Websites" section. It is highly recommended that you do not allow any games to have access to your Facebook account.



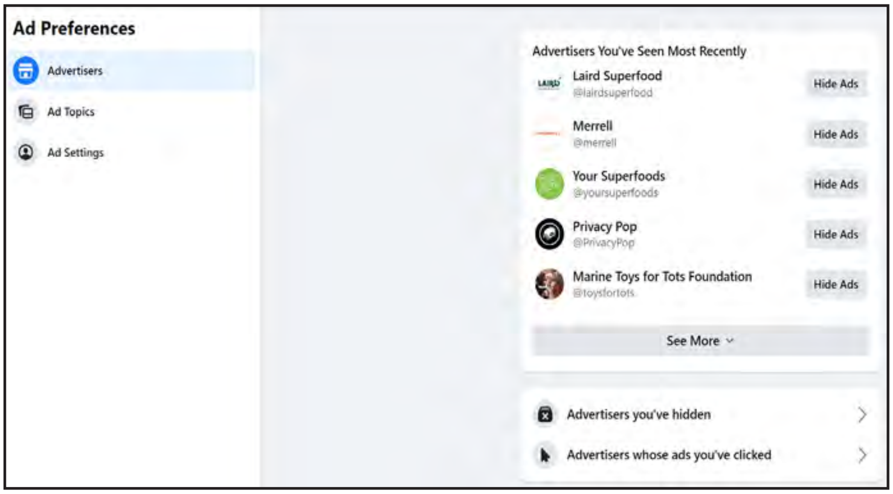
Instant Games

These are Instant Games you've played on Facebook or Messenger. They can receive information you chose to share with them. Expired and removed apps may still have access to information that was previously shared with them, but can't receive additional non-public information. Learn More

Manage what information you're sharing or remove any Instant Games that you no longer want to use.

WOW
Added on Apr 23, 2020

Facebook just recently changed their "Ads Preferences," it is now more in-depth and requires attention. On the left side "Settings" menu select "Ads" where you will be redirected to the "Ads Preference" section. This section is a bit more detailed than it first lets on. Each section here will need your attention starting with the "Advertisers" section. Here you can review ads you have recently seen on Facebook and decide whether you want to be seeing them in the future. Once you have gone through this list head to the left and select "Ad Topics" from the side menu. Here you can manage which ad topics you want to be seeing and not seeing. Next (and most importantly) head to the "Ad Settings" section from the left menu. In this section you can manage where Facebook allows ads to pull information from about you. This section can be a bit cumbersome, be sure to go through each subsection here starting with "Data about your activity from partners." It is recommended that you do not allow Facebook to personalize ads for you on any account you may have linked to Facebook (which is hopefully just Facebook). Next in "Categories used to reach you" it is recommended that you toggle each section to off so that Facebook ads cannot use your personal information to provide Ads to you. In this same section it is also important to review the "Interest Catego-



Ad Preferences

Advertisers
Ad Topics
Ad Settings

Advertisers You've Seen Most Recently

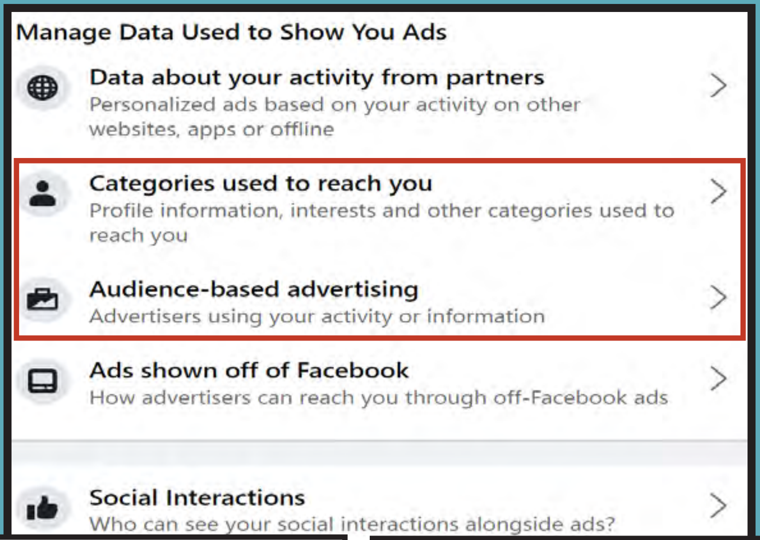
Laird Superfood @lairdsuperfood	Hide Ads
Merrell @merrell	Hide Ads
Your Superfoods @yoursuperfoods	Hide Ads
Privacy Pop @PrivacyPop	Hide Ads
Marine Toys for Tots Foundation @toysfortots	Hide Ads

See More
Advertisers you've hidden
Advertisers whose ads you've clicked

> Some users are so overwhelmed by the curiosity that they tend to ignore some of the risks involved, and inadvertently give the app access to sensitive data. Never give up too much information, drawing out your family members on Facebook could help an Identity Thief answer security questions about you. #themoreyouknow

ries" and the "Other Categories" both of which have additional information to be reviewed and locked down. Now, select "Audience-based advertising" to review each advertiser that uses your information to push your ads. Here, unfortunately you will need to go through each listed advertiser who is using your information. Select the advertiser then select the section under "Why are you in this advertiser's audience?" and select "Don't Allow" (shown already selected to the right highlighted in red) in each section where it is permitted. Finally, select "Ads shown off of Facebook" where it is recommended you select "Not Allowed" in order to prevent advertisers from pushing ads to you off of Facebook.

Now that you have completed the "Settings" sections, let us move on to secure your personal profile information. First, from the "Home" screen, select your "Profile Picture" or "Username". Next, select "About" on your personal "Profile Page". You should go through each selection in the "About" section and make sure the privacy settings are as secure as possible. You will see two update opportunities for each item: First:) privacy, and Second:) edit. We recommend you choose "Only Me" as much as possible, and "Friends" as a second choice for who each piece of information is presented to. When "editing", remember to include the least amount of information possible wherever you can, leave your inputs blank, and where you provide information, keep it vague.



Manage Data Used to Show You Ads

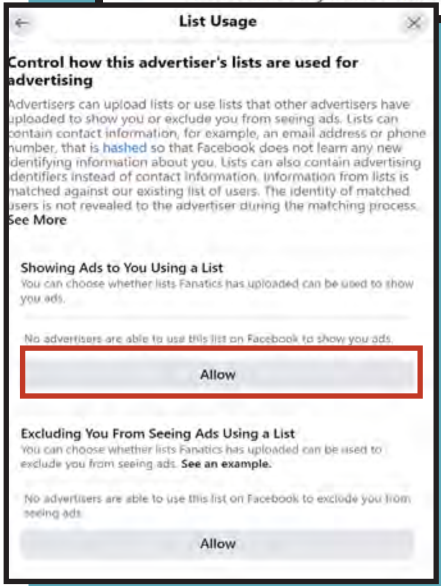
Data about your activity from partners
Personalized ads based on your activity on other websites, apps or offline

Categories used to reach you
Profile information, interests and other categories used to reach you

Audience-based advertising
Advertisers using your activity or information

Ads shown off of Facebook
How advertisers can reach you through off-Facebook ads

Social Interactions
Who can see your social interactions alongside ads?



List Usage

Control how this advertiser's lists are used for advertising

Advertisers can upload lists or use lists that other advertisers have uploaded to show you or exclude you from seeing ads. Lists can contain contact information, for example, an email address or phone number, that is hashed so that Facebook does not learn any new identifying information about you. Lists can also contain advertising identifiers instead of contact information. Information from lists is matched against our existing list of users. The identity of matched users is not revealed to the advertiser during the matching process. See More

Showing Ads to You Using a List
You can choose whether lists Fanatics has uploaded can be used to show you ads.

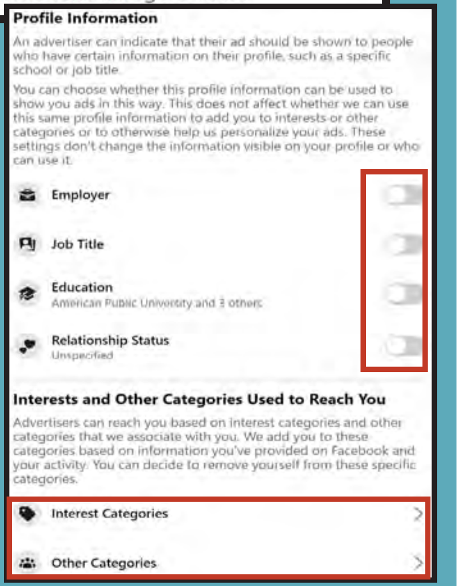
No advertisers are able to use this list on Facebook to show you ads.

Allow

Excluding You From Seeing Ads Using a List
You can choose whether lists Fanatics has uploaded can be used to exclude you from seeing ads. See an example.

No advertisers are able to use this list on Facebook to exclude you from seeing ads.

Allow



Profile Information

An advertiser can indicate that their ad should be shown to people who have certain information on their profile, such as a specific school or job title.

You can choose whether this profile information can be used to show you ads in this way. This does not affect whether we can use this same profile information to add you to interests or other categories or to otherwise help us personalize your ads. These settings don't change the information visible on your profile or who can use it.

Employer

Job Title

Education
American Public University and 3 others

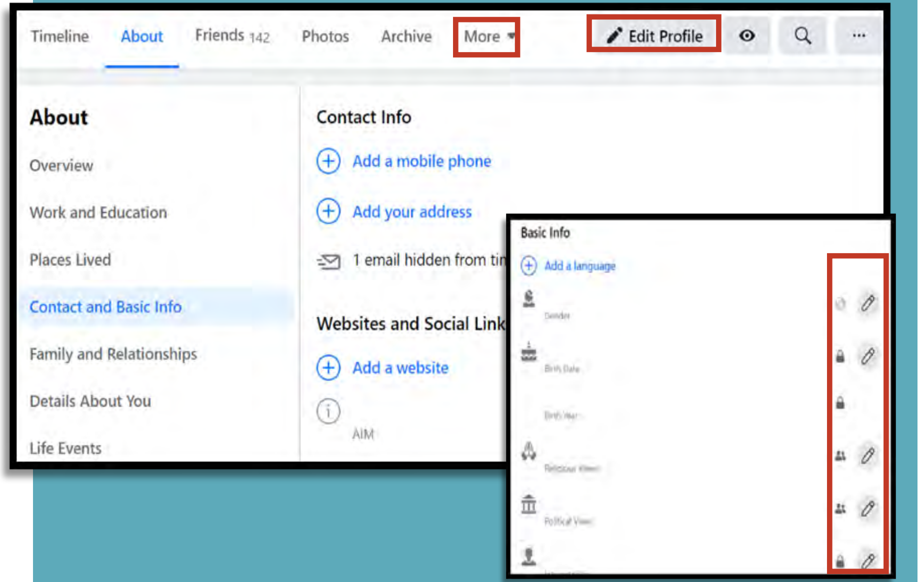
Relationship Status
Unspecified

Interests and Other Categories Used to Reach You

Advertisers can reach you based on interest categories and other categories that we associate with you. We add you to these categories based on information you've provided on Facebook and your activity. You can decide to remove yourself from these specific categories.

Interest Categories

Other Categories



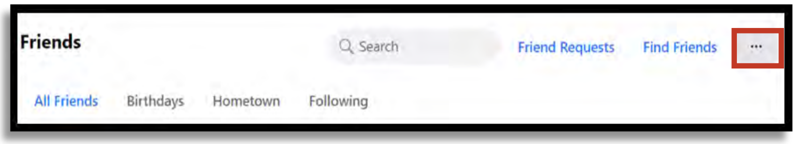
About
Overview
Work and Education
Places Lived
Contact and Basic Info
Family and Relationships
Details About You
Life Events

Contact Info
Add a mobile phone
Add your address
1 email hidden from ti

Websites and Social Link
Add a website
AIM

Basic Info
Add a language
Gender
Birth Date
Birth Year
Religious Views
Political Views

*Social Engineers or Human Hackers are more likely to convince you that they know you if they have access to personal information about you. This information can be in the form of your likes/hobbies, friends, events you will or have been to or what schools you have previously attended. They can even review past posts you may have open to the public for some additional insight. Once they have convinced you that you are "old friends" there is significant danger. They could convince you to meet in person, lend them money, steal your identity, or get close to your children. The best defense is to limit who can see this information about you to "Only Me" or "Friends".

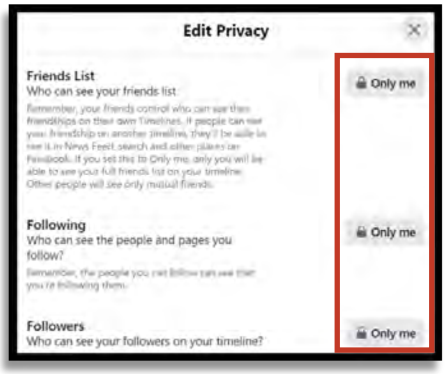


Friends

Search · Friend Requests · Find Friends · ···

All Friends · Birthdays · Hometown · Following

Below this, is your "Friends" section. Here, select the "Options", or " . . ." button in the upper right corner of the section. Select "Edit Privacy" (not shown, but only option), then adjust the settings in the pop-up box (see right). We recommend setting all three options to "Only Me".



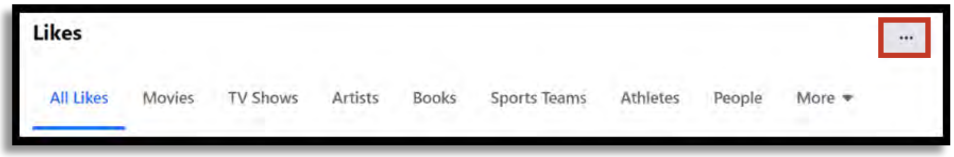
Edit Privacy

Friends List
Who can see your friends list
Remember, your friends control who can see their friendships on their own Timelines. If people can see your friendship on another timeline, they'll be able to see it in News Feed, search and other places on Facebook. If you set this to Only me, only you will be able to see your full friends list on your timeline. Other people will see only mutual friends.
Only me

Following
Who can see the people and pages you follow?
Remember, the people you [illegible] follow can see that you're following them.
Only me

Followers
Who can see your followers on your timeline?
Only me

The things you "Like" on Facebook can be analyzed in order to create an accurate profile of you. This information can be a lot more dangerous than you might imagine. In the "About" section, you can control who sees your "Likes" by selecting the "…" button to the right of each interest category (e.g.: sports, music), then select "Edit Privacy", and set your "Likes Privacy" icon to "Only Me" or "Friends" on each section. "Only Me" is the most secure choice and recommended whenever possible.

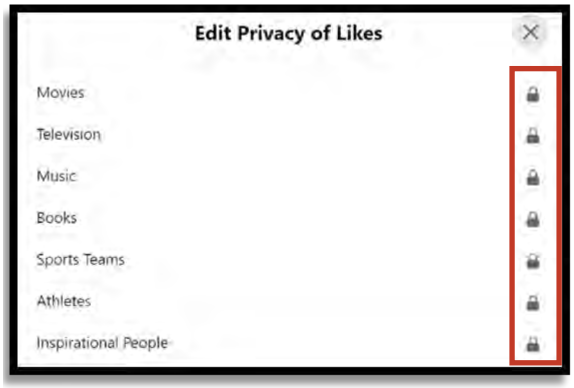


Likes

···

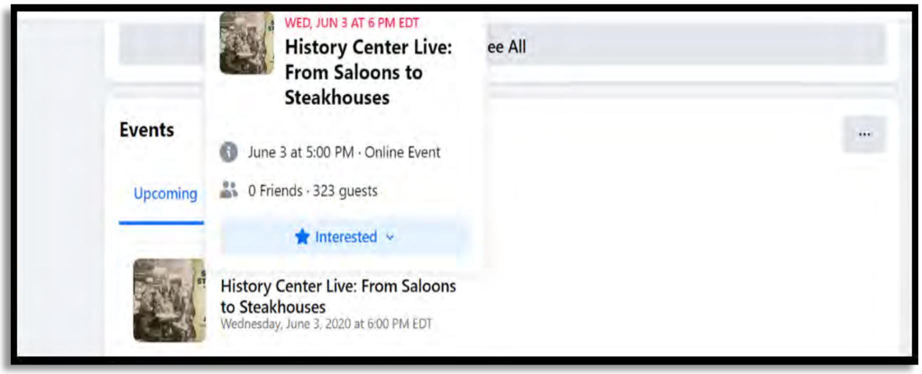
All Likes · Movies · TV Shows · Artists · Books · Sports Teams · Athletes · People · More ▾

Although you have enhanced the security of your "Likes" above, you will need to repeat the process in each section that is currently visible on your profile or your can head back up to the Profile header menu (shown on the previous page) and select "More" then select "Manage Sections." If you do not need necessarily need people to be able to view your "Like" it is highly recommended that all "Likes" sections be "Only Me" in order to prevent unknown users from gaining information abouot you.



Edit Privacy of Likes

Movies 🔒
Television 🔒
Music 🔒
Books 🔒
Sports Teams 🔒
Athletes 🔒
Inspirational People 🔒



Events

Upcoming

WED, JUN 3 AT 6 PM EDT
History Center Live: From Saloons to Steakhouses
June 3 at 5:00 PM · Online Event
0 Friends · 323 guests
★ Interested ⌄

History Center Live: From Saloons to Steakhouses
Wednesday, June 3, 2020 at 6:00 PM EDT

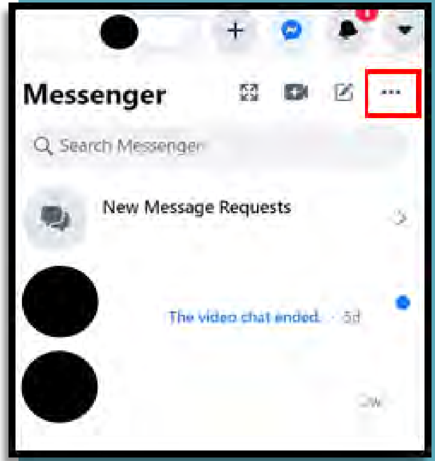
ee All

···

Next, as you continue to scroll down the page, you may want to go through all your "Events" to see if there are any you can delete. Also, make sure all your events are set to "Only Me" by hovering over the event title, clicking the "Going" button, and looking to the bottom line of the pop-up for "Visible to the Hosts and Only Me" (not shown). If you have an upcoming "Event" or an "Event" that you are "interested in" that is not set to "Only Me", be aware that anyone will be able to see that you will be attending that event. You also have the option of hiding the entire 'Events" section. Go to the " . . ." button at the top right corner of the "Events" section, select "Hide Section". This is the quickest and easiest way to secure this information and is what we recommend. Remember to do this in both "Upcoming" and "Past" sections. It is equally important to ensure you "hide" and lock down your "Check-ins" if they are showing as well as your "Reviews." These three "Sections" create a past, present, and future pattern of life on an individual.

Think
once before you act
twice before you speak
and three times
before you post
on Facebook

Next is the "Messenger" feature, there are a few things to cover in order to protect your privacy here. First, go to the top of the page to the "Messenger" icon, and see the "Messenger" dropdown. Here you will be able to turn "On" and "Off" your "Status" on "Messenger". Select the ". . ." button, then select "Turn Off Active Status". Choose one of the three options on the pop-up screen and select "Okay". In this way, you can control who, if anyone, can see that you are actively using Facebook at any given time.



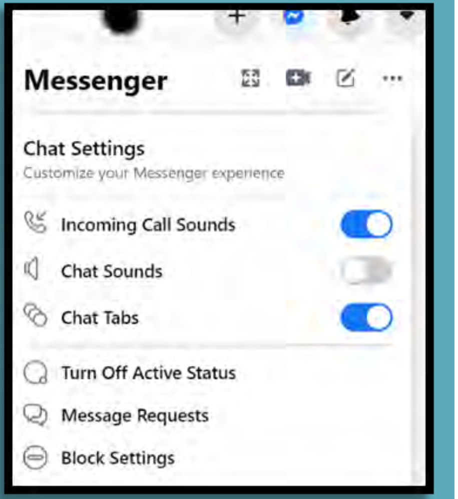
Messenger

Search Messenger

New Message Requests

The video chat ended. · 5d

2w



Messenger

Chat Settings

Customize your Messenger experience

Incoming Call Sounds

Chat Sounds

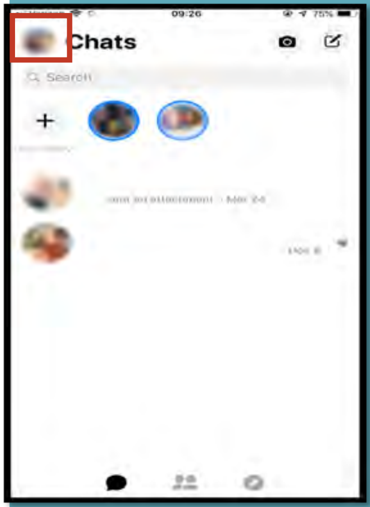
Chat Tabs

Turn Off Active Status

Message Requests

Block Settings

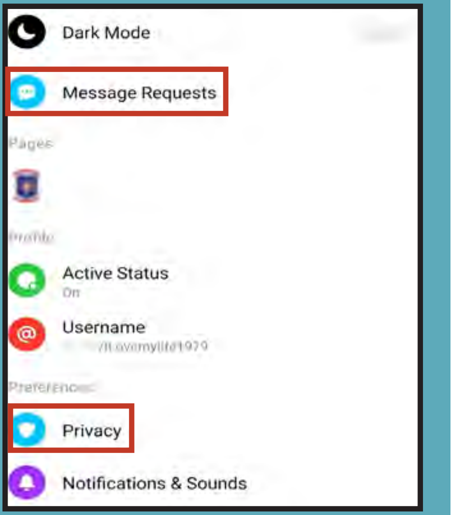
The final section you may want to review on Facebook is your "Messenger" (computer based or application), though this information mainly applies to your mobile device both computer based and application are equally as important to periodcially review. Facebook launched a dedicated website interface and separated its messaging functionality from the main Facebook app, allowing users to use the web interface or download one of the standalone apps. What this means for you is that you may be taken outside of Facebook sometimes, when you are trying to access Facebook "Messenger". Also, your computer version of "Messenger" may look different from your mobile device version and will have less features. It is important to look over and go through both the computer based and mobile based applications.



09:26

Chats

Search



Dark Mode

Message Requests

Pages

Profile

Active Status

On

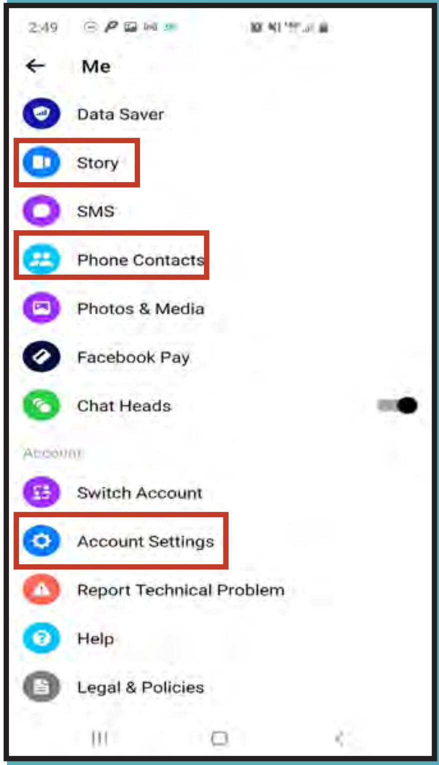
Username

Preferences

Privacy

Notifications & Sounds

Once logged into Facebook "Messenger", head to the top left of the screen, select your "Profile Picture" (highlighted above in red). Here you can review all the additional settings "Messenger" has to offer. We recommend reviewing and updating the "Privacy" section on Messenger periodically. Here users can turn on and off "Secret Conversations" and select the audience they want their "Stories" to reach. Once you have updated your "Privacy" settings go back to the main settings page and review your "Phone Contacts" to make sure you didn't inadvertently allow Facebook access to your contacts. You can also review "Message Requests" and "Account Settings" for Facebook right from your Messenger. You can also review your "Account Settings" (e.g.: personal info, privacy, ads) on Facebook from this appication, again periodically this is a good idea just as a check up.



2:49

Me

Data Saver

Story

SMS

Phone Contacts

Photos & Media

Facebook Pay

Chat Heads

Account

Switch Account

Account Settings

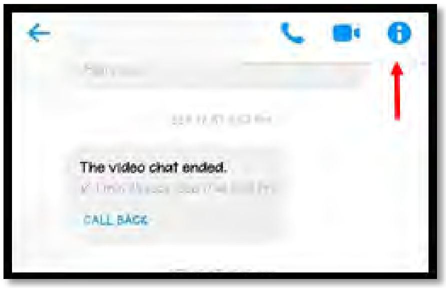
Report Technical Problem

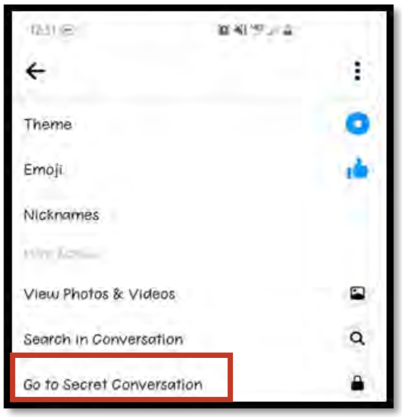
Help

Legal & Policies

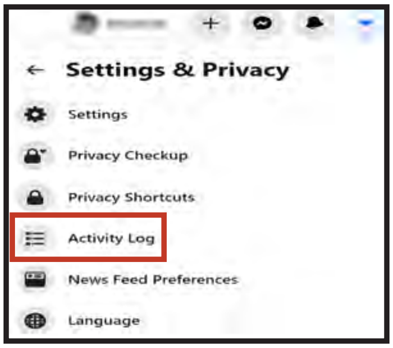
Facebook "Messenger" has a feature called "Secret Conversations" where your conversations are encrypted end-to-end. Once you have turned this function on it is important to note that it will remain on (*New Facebook Feature*). If you wish to make a conversation "Secret" you can do so one of two ways: First is to go into the specific chat you wish to make secret and select the "information" icon in the upper right hand corner (shown to the

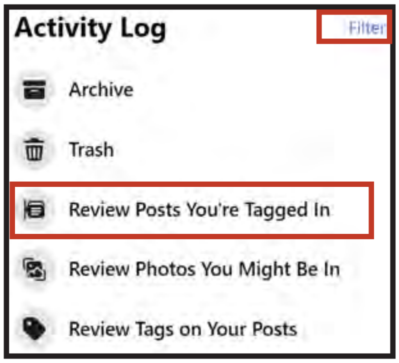
FACEBOOK SMARTCARD



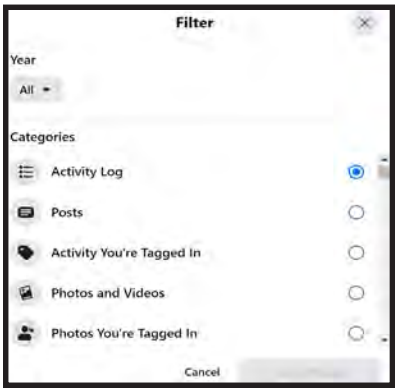


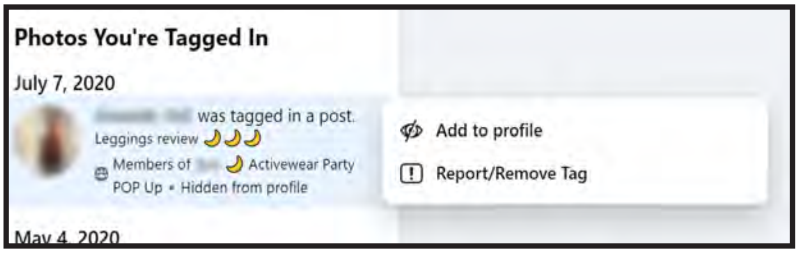
left here), then select "Go to Secret Conversation." The second way to turn this feature on is to go back to your Messenger main menu (shown on the previous page) and select "Privacy," then select "Secret Conversations." If you do not want all conversations to be encrypted in this way it is recommended you go in to specific conversations and turn on "Secret Conversations" that way. Also, if you have children that use Facebook Messenger, it is important to know about this feature so you can monitor it as you see fit.

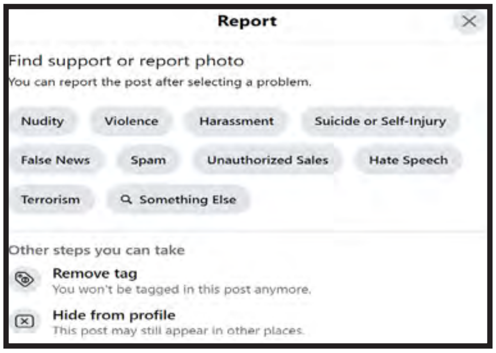



Activity Log
Filter
Archive
Trash
Review Posts You're Tagged In
Review Photos You Might Be In
Review Tags on Your Posts

Finally, let's go back to Facebook's "Activity Log", accessed from the "Settings & Privacy" option under the "Down Arrow" in the right upper corner of the "Home Page". The "Activity Log" allows you to review any click of the button (photos, comments, Likes, posts, etc.) or tag that has ever occurred and been associated with your profile. This is the central location for cleaning up your Facebook profile. More specifically, from the "Activity Log" you can review information by date, all the way from the creation of the profile to the present. You can also see if a post is viewable to the public or just to friends, as well as review any posts you have been "Tagged" in. Finally, the "Activity Log" allows you to remove any actions you have taken on Facebook as well as any "Tags" that someone else may have posted.



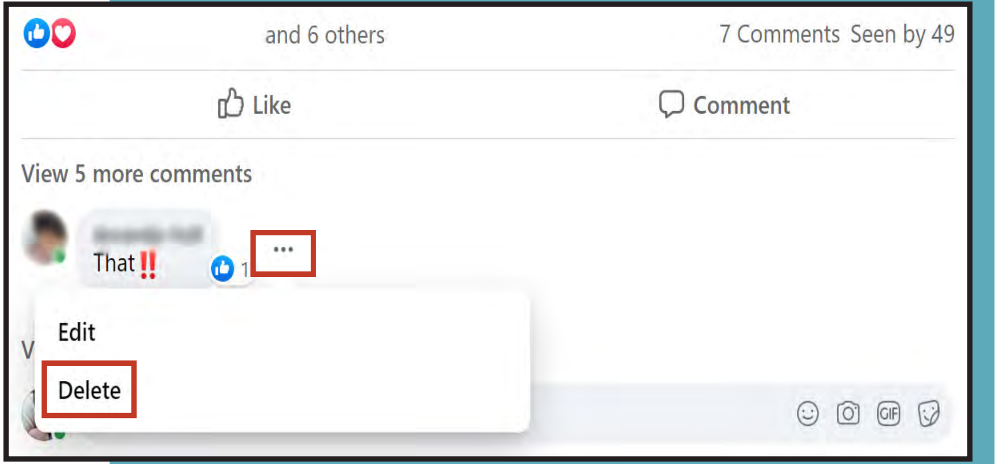




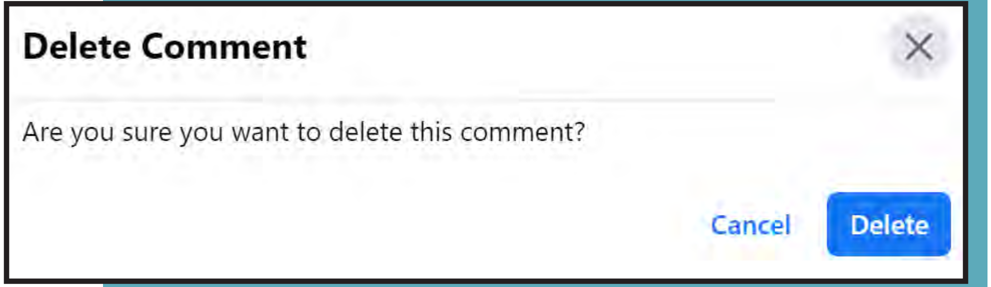
Facebook recently changed the "Activity Log" page so the view you now see may be a little different than before. After selecting "Activity Log" from the "Settings" menu, look to the left side of your screen, here you can select "Filter" or you can simply select one of the pre choice selections Facebook has provided to you (see picture on the left marked Activity Log). If you select "Filter" and at some point you will want to go through all the filters, you can select whichever filter you wish to review at this time and then hit "Save Changes." Once you have the "filter" you wish to review selected you will find below the "Activity Log" menu, a list that contains all the items related to your designated filter. From there you can scroll through the list and if you happen to come across an item you wish to remove such as a photo you are tagged in you can remove it. Hover over the post you wish to remove yourself from and select the menu on the right (three dots), now select "Report/Remove Tag" and then select "Remove Tag" as shown on the previous page. It is highly recommended you go through each filter at least once; you can also select the "Activity Log" setting under filter and it will show you all the filters all at once.

Don't think you can hide your FB profile by using a different name. Better to assume people can find you and set your privacy/security settings accordingly. Likewise, correcting posts might be tempting, but think about what correcting that post says about you and the information you have access to.

From the "Activity Log" you can also change the "audience" you have designated on a post, however unlike the previous instructions, you must select the post and then select the menu (three dots) from the middle of your screen and not the side view, then simply select "Edit audience." Remember if you "Like" or "Comment" on someone else's post whose privacy settings are set to "Public", your comment will also be "Public". You can only set your own privacy settings for your profile, and once you reach outside of your profile, you have no control over privacy. If you are reviewing your "Activity Log" for the first time you may find comments you have previously made that, now do not wish to be visible. These comments can be removed from the post in the same way you previously removed photos, likes or will soon remove tags.



Finally, let's address "Tags", which are a feature of Facebook by which other people can call attention to your name by "Tagging" a photo that you may or may not be in, or "Mentioning" you in a "Post" or "Comment". People can do this without your permission if you don't have the "Tagging" options selected as we have done in this Card. When you are "Tagged" in a photo, that photo is viewable by the "Public", while also drawing attention to your name. Here is what you can do about it.



Are you sure you want to delete this comment?

First, in "Activity Log", select "Tag Review", then select "Activity You're Tagged In". All the "Posts", "Comments", and photos you are tagged in appear in the left column. Select the "Post" you want to view and "Untag". The post will open in the box to the right of the screen. Select the " . . ." in the right upper corner of the post, and select "Remove Tag" on the drop-down. Note: If you remove a "Tag" of yourself, it will NOT notify the individual who owns the post/picture that you have removed the tag.

Remember: Although the photo is "Untagged" and no longer on your profile, the photo has not been deleted from Facebook. It will remain on the profile of the individual who originally posted the photo. Backdoor avenues used in finding your profile may still exist (e.g. via a tagged photo of you on your spouse's profile or simply finding your name in the comments of the picture/post). If you would like for the photo to be removed, the best way is to ask the individual to delete the photo/post. If f for some reason the individual who posted the photo refuses to remove the photo you can ask Facebook to remove it for you, so long as your reasoning fits one of their categories for removal.

FACEBOOK SMARTCARD

HACKED

- Do you think your account may have been compromised or hacked? Have you noticed any of the following:
- Unexpected posts posted by your account
- Any Direct Messages sent from your account that you did not initiate
- Other account behaviors you didn't perform or approve (like following, unfollowing, blocking, etc.)
- A notification from Facebook stating that your account may be compromised
- A notification from Facebook stating that your account information (bio, name, etc.) has changed
- Your password is no longer working or you are being prompted to reset it. *If this occurs it is highly recommended that you sign-in online and change your password immediately.

- If you said "Yes" to any of the above , it is advised you take the following actions:
- Delete any unwanted posts that were posted while your account was compromised
- Scan your computers for viruses and malware, especially if unauthorized account behaviors continue to be posted after you've changed your password
- Make sure to change your password. Always use a strong password you haven't used elsewhere and would be difficult to guess
- Consider using login verification (if you haven't done so already), instead of relying on just a password. Login verification introduces a second check to make sure that you and only you can access your Facebook account
- Be sure to check that your email is secure. It may be worth changing the password to both your Facebook account and the email associated with your Facebook account. *If you feel your email may have been compromised and need help finding the right contact information for your email provider please see page 21 of this smart book under the "blue box" at the bottom of the page.

If you need to report Spam/Harassment: Go to https://www.facebook.com/help/968185709965912/?helpref=hc_fnav

If your account was hacked: https://www.facebook.com/help/hacked
Also, if you find that someone is impersonating you Facebook: https://www.facebook.com/help/hacked then scroll down to the "Impersonation Accounts" section and follow the directions. If you do not have a Facebook account and want to report an impersonating account go to: https://www.facebook.com/help/contact/295309487309948

To find additional "Security Features and Tips go to: https://www.facebook.com/help/379220725465972?helpref=faq_content

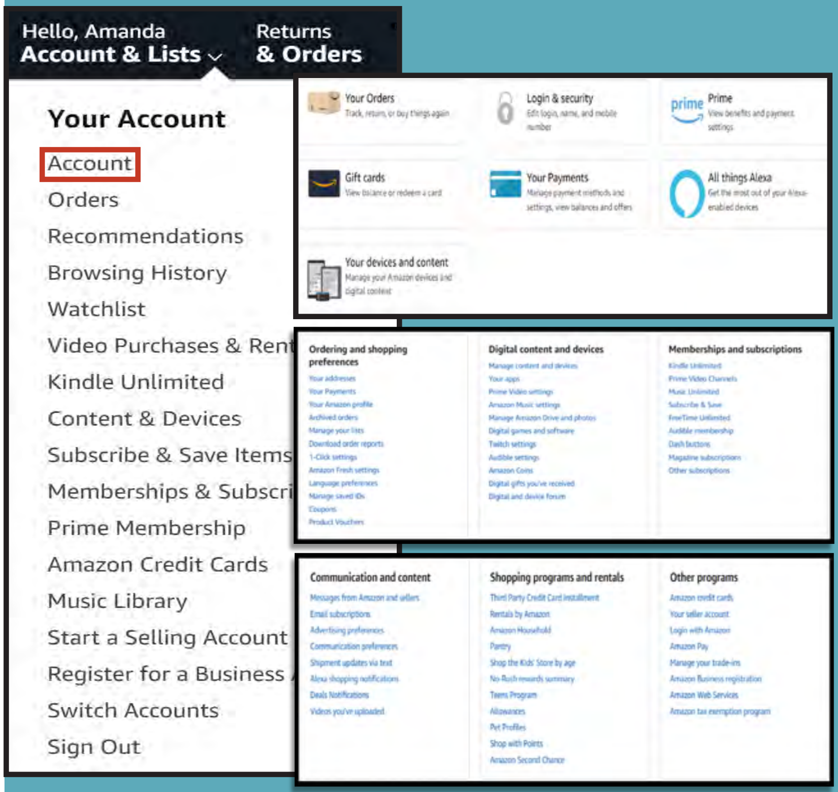
If you still need help or have questions, you can always contact Facebook by: https://www.facebook.com/facebookapp where you can message a Bot Facebook created to help answer questions while they work on building a live customer support capability.

If someone is threatening to share information (ex: messages or photos) on Facebook of your child that they do not want shared you should report it to the local law enforcement. Facebook also says you can do the following: Report the incident to Facebook https://www.facebook.com/help/contact/567360146613371, then make sure that this person is blocked so they no longer have access to your child. It is important to talk to your children about this possibility before they begin to use social media so that they know what to do should this happen to them.

AMAZON SMARTCARD

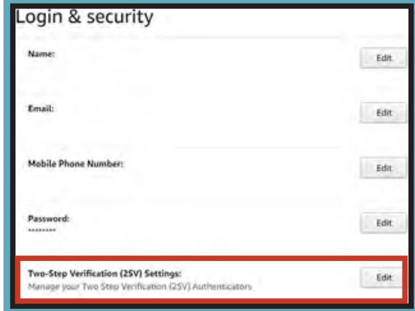
PERSONAL COMPUTER (PC) VERSION

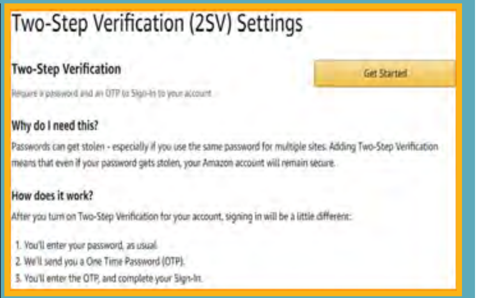
In order to lock down your Amazon account you will need to access "Your Account," located on the upper right side of your screen. You will notice, to the right, a visual representation of the Amazon Drop down menu and all three sections within the "Account" section. Each of these sections will be noted periodically throughout this guide please take note of them here as a reference point.



Looking towards the upper right of your screen, see "Account & Lists" and select the down arrow. From this list, select "Account."

Let's look at the "Login & Security" settings first. The "Login & Security" settings are located in the first section of the "Account" page. First, review the general login information provided to ensure its accuracy. Next, head to the "Two-Step Verification (25V) Settings" section and select "Edit." Now, select "Get Started" (highlighted in red to the right) and follow the steps provided. Because Amazon retains some of your most sensitive information, like your credit cards and address, this feature is important to help secure your account. Here, you can set up "Two-Step Verification" for your account. It is highly recommended throughout this guide that, where possible, you turn on "Two-Step Verification" in order to help prevent others from gaining access to your account.


Login & security
Name:
Edit
Email:
Edit
Mobile Phone Number:
Edit
Password:
****
Edit
Two-Step Verification (2SV) Settings:
Manage your Two Step Verification (2SV) Authenticators
Edit



Two-Step Verification (2SV) Settings

Two-Step Verification

Get Started

Require a password and an OTP to Sign-In to your account

Why do I need this?

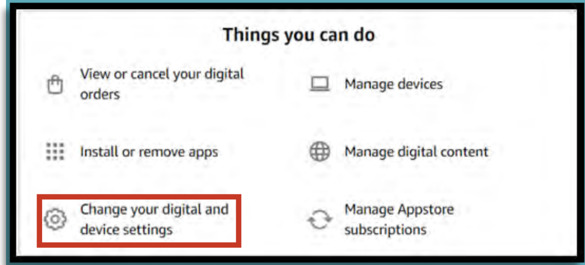
Passwords can get stolen - especially if you use the same password for multiple sites. Adding Two-Step Verification means that even if your password gets stolen, your Amazon account will remain secure.

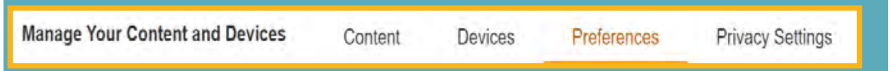
How does it work?

After you turn on Two-Step Verification for your account, signing in will be a little different:

1. You'll enter your password, as usual.
2. We'll send you a One Time Password (OTP).
3. You'll enter the OTP, and complete your Sign-In.

Now, let's go back to the "Account" page and select "Your devices and content", then select "Change your digital and device settings" which will likely open up to the "Preferences" section if not select "Preferences" from the top menu. You may want to review the settings to make sure the content agrees with your needs. We recommend that you review "Saved Wi-Fi Passwords" to make sure there are no passwords saved that you do not want Amazon to retain. There is a plethora of other settings to check within this section and it is recommended periodically that users revisit this site to ensure all settings have remained intact.

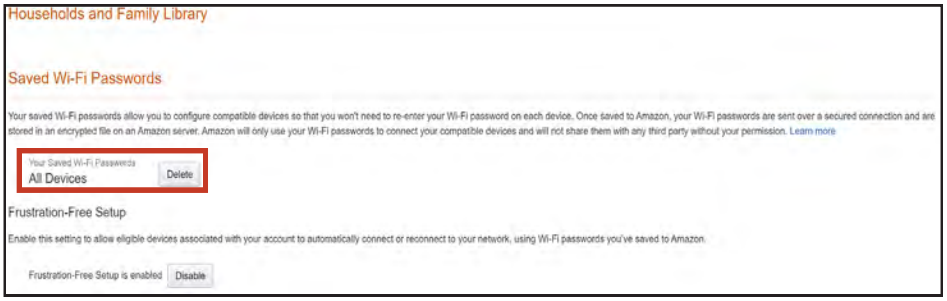

Things you can do
View or cancel your digital orders
Manage devices
Install or remove apps
Manage digital content
Change your digital and device settings
Manage Appstore subscriptions



- Do take time to clean up old credit cards from your account.
- Do use Two-Factor Authentication to protect all your information on Amazon. With all the information that Amazon captures it is important to make sure it is protected by every means available.
- Do frequently update your password for Amazon.

- Do not link any other accounts to your Amazon account. This will limit what outsiders can find out about you, to include your pattern of life and hobbies.
- Do not fall for scams on Amazon or from emails that appear to be from Amazon.
- Do not buy from international sellers. Avoiding this will help protect you from identity theft and scams.

AMAZON SMARTCARD



Households and Family Library

Saved Wi-Fi Passwords

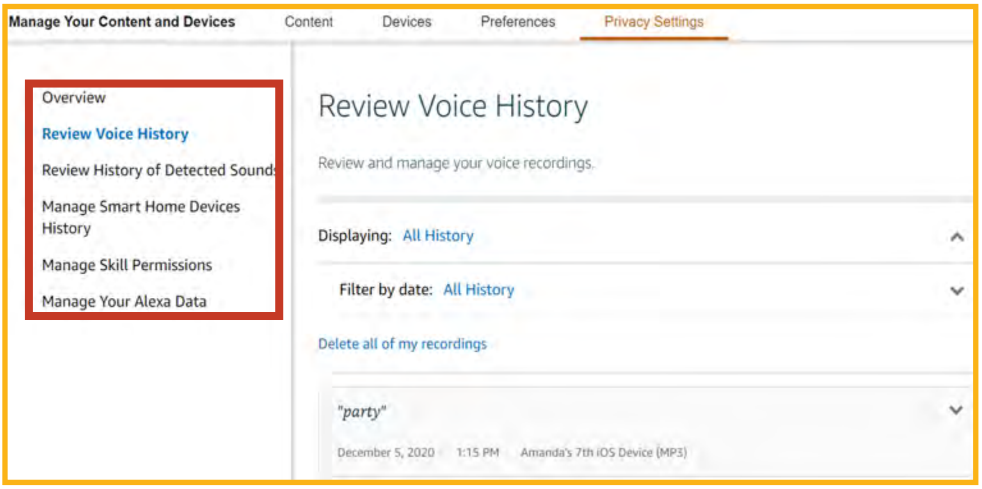
Your saved Wi-Fi passwords allow you to configure compatible devices so that you won't need to re-enter your Wi-Fi password on each device. Once saved to Amazon, your Wi-Fi passwords are sent over a secured connection and are stored in an encrypted file on an Amazon server. Amazon will only use your Wi-Fi passwords to connect your compatible devices and will not share them with any third party without your permission. Learn more

Your Saved Wi-Fi Passwords
All Devices

Frustration-Free Setup

Enable this setting to allow eligible devices associated with your account to automatically connect or reconnect to your network, using Wi-Fi passwords you've saved to Amazon.

Frustration-Free Setup is enabled



Review Voice History

Review and manage your voice recordings.

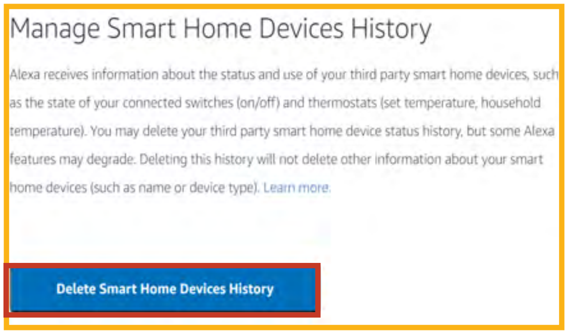
Displaying: All History

Filter by date: All History

Delete all of my recordings

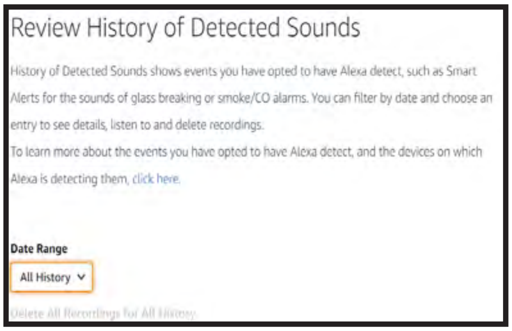
"party"

December 5, 2020 1:15 PM Amanda's 7th iOS Device (MP3)



Manage Smart Home Devices History

Alexa receives information about the status and use of your third party smart home devices, such as the state of your connected switches (on/off) and thermostats (set temperature, household temperature). You may delete your third party smart home device status history, but some Alexa features may degrade. Deleting this history will not delete other information about your smart home devices (such as name or device type). Learn more.



Review History of Detected Sounds

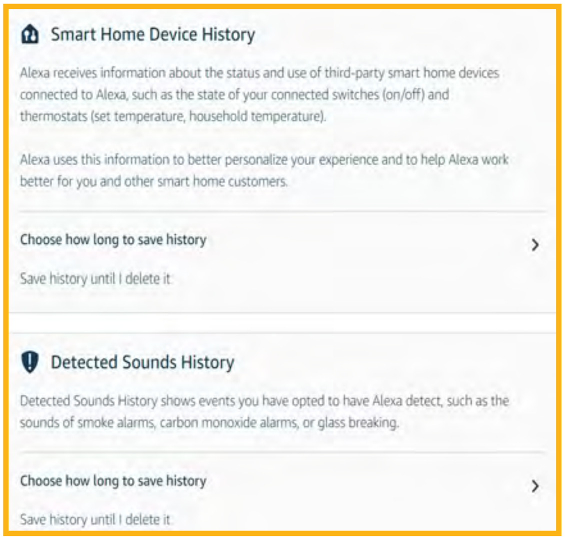
History of Detected Sounds shows events you have opted to have Alexa detect, such as Smart Alerts for the sounds of glass breaking or smoke/CO alarms. You can filter by date and choose an entry to see details, listen to and delete recordings.

To learn more about the events you have opted to have Alexa detect, and the devices on which Alexa is detecting them, click here.

Date Range

All History

Delete All Recordings for All History



Smart Home Device History

Alexa receives information about the status and use of third-party smart home devices connected to Alexa, such as the state of your connected switches (on/off) and thermostats (set temperature, household temperature).

Alexa uses this information to better personalize your experience and to help Alexa work better for you and other smart home customers.

Choose how long to save history

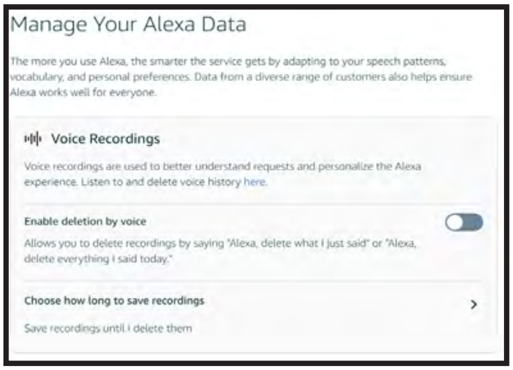
Save history until I delete it

Detected Sounds History

Detected Sounds History shows events you have opted to have Alexa detect, such as the sounds of smoke alarms, carbon monoxide alarms, or glass breaking.

Choose how long to save history

Save history until I delete it



Manage Your Alexa Data

The more you use Alexa, the smarter the service gets by adapting to your speech patterns, vocabulary, and personal preferences. Data from a diverse range of customers also helps ensure Alexa works well for everyone.

Voice Recordings

Voice recordings are used to better understand requests and personalize the Alexa experience. Listen to and delete voice history here.

Enable deletion by voice

Allows you to delete recordings by saying "Alexa, delete what I just said" or "Alexa, delete everything I said today."

Choose how long to save recordings

Save recordings until I delete them

Now look to the "Manage Your Content and Devices" header menu and select "Privacy Settings" and either select "Alexa Privacy" from the drop menu or simply select the full menu and then select "Alexa Privacy." Here users can review the privacy settings associated with any of their Alexa devices. First look to the right (shown here to the left) to find the "Alexa Privacy" menu and select "Review Voice History." Here you can review every sound detected by Alexa, which includes but is not limited to you any and all commands you have ever ask of Alexa. It is recommended that periodically users visit this section and clear your command history the same way you would clear your cookies and cache from the internet. Select the time frame you wish to review/delete and then select "Delete Detected Sounds History." Next, locate "Review History of Detected Sounds" from the side menu to review any sound Alexa may have picked up over the course of her "life". It is recommended here also that this section be periodically deleted. Now, select "Review Smart Home Devices History" here users can review all devices that are connected to Alexa, which also means they are connected to Amazon and can potentially make purchases on that connected account. This section should be reviewed quarterly to ensure only trusted devices are connected to Alexa and all others are deleted. In the next section, "Manage Skill Permissions," users can review any "skills" they may have enabled Alexa to have, such as accessing a devices street address or email address. It is not recommended that any of these "skills" be enabled. Finally, select "Manage Your Alexa Data" and review any information here that you do not wish Alexa to have or you can set how long information such as recordings are kept. Once you have completed this section head back to the main Account section (shown again on page one of this guide).

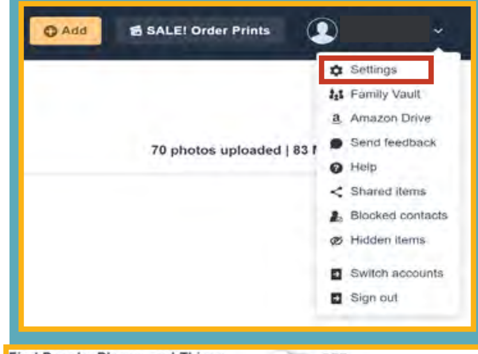
Each Amazon account comes with an "Amazon Drive". In order to lock down your "Amazon Drive," look to the second section on your "Account" and se-

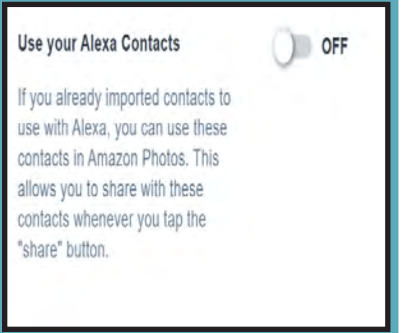
You can call the customer service department and ask about suspicious emails to see if it's authentic. Whatever you do, don't try to get to Amazon through the suspicious email. If you need to contact Amazon's customer service make sure to find the number from the official Amazon site. Searching for it online could lead to you providing information to a fake call center.

lect “Manage Amazon Drive and Photos.” On the top right of the screen, select the profile picture to open the “Drive” menu. Next, select “Settings” and review each section present on your screen. It is important to note there is a new section titled “Use your Alexa Contacts.” It is not recommended that users allow Alexa to obtain access to your contacts, be sure this function is “off”. Other sections to be sure and visit here are “Find People, Places, and Things,” “Add Uploads to Family Vault” as well as the “Manage Third-Party Apps” section located at the bottom of the screen (noted to the right of this page). Once there, select “Manage Login with Amazon.” Here you can review any apps you may have logged on to through your Amazon account and if need-be, remove accounts you no longer use.

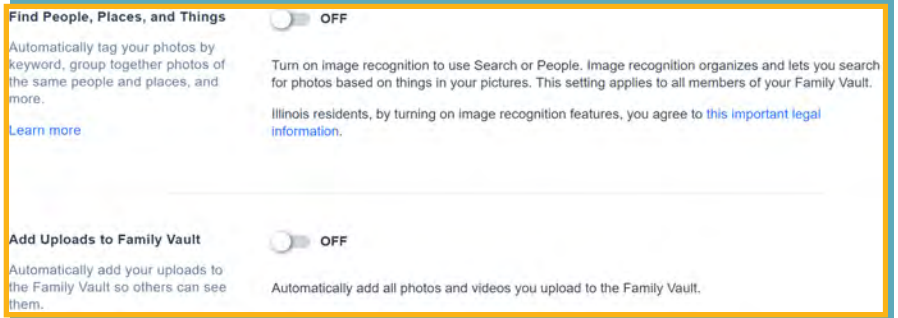
Most people do not realize that Amazon provides you with your own “Public Profile”. This “Profile” and your entire “Amazon Account” can be linked to any of your social media accounts. It is therefore important to review your profile and its settings to ensure it is locked down, not linked to other social media accounts, and not searchable by the public.
In order to lock down your Amazon account, go back to “Your Account”, select “Your Name’s Amazon.com”, the second item on the second menu bar, then “Your Profile” on the third menu bar that appears (see above). From there, follow the steps below and on the remaining pages to best secure your profile.

Now let’s begin the process of making sure your “Profile” is locked down. Select “Edit your profile” as shown above in red. In the “Profile page settings” review all your information to make sure only information you want on public profile is filled in. We recommend you not display your full name in the “Your public name” section. Scroll down on the page and find the “Add social links to your profile” section to make sure you have not linked any of your social media accounts to your Amazon account. Amazon is a great place to shop for just about anything, and as such it becomes a picture of who you are and who your family might be. This includes any product reviews you post on Amazon. It is recommended that if you do review products, that you do not put any personal information in your review.




Use your Alexa Contacts — OFF

If you already imported contacts to use with Alexa, you can use these contacts in Amazon Photos. This allows you to share with these contacts whenever you tap the "share" button.


Find People, Places, and Things — OFF

Automatically tag your photos by keyword, group together photos of the same people and places, and more.
Learn more

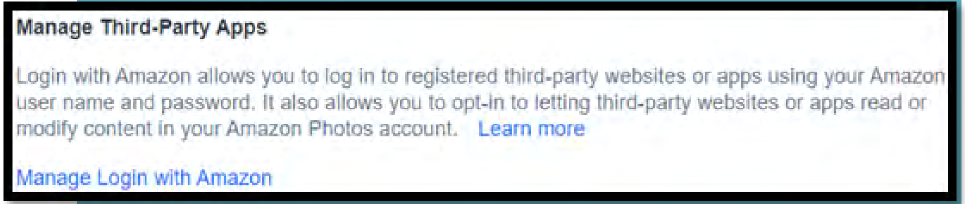
Turn on image recognition to use Search or People. Image recognition organizes and lets you search for photos based on things in your pictures. This setting applies to all members of your Family Vault.

Illinois residents, by turning on image recognition features, you agree to this important legal information.

Add Uploads to Family Vault — OFF

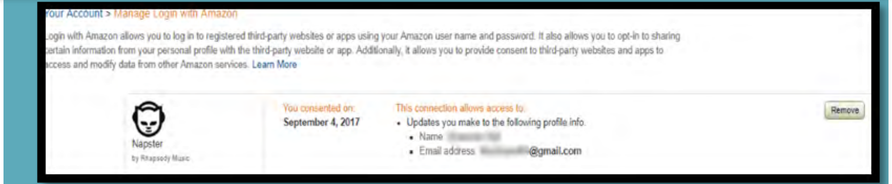
Automatically add your uploads to the Family Vault so others can see them.

Automatically add all photos and videos you upload to the Family Vault.


Manage Third-Party Apps

Login with Amazon allows you to log in to registered third-party websites or apps using your Amazon user name and password. It also allows you to opt-in to letting third-party websites or apps read or modify content in your Amazon Photos account. Learn more

Manage Login with Amazon


Your Account > Manage Login with Amazon

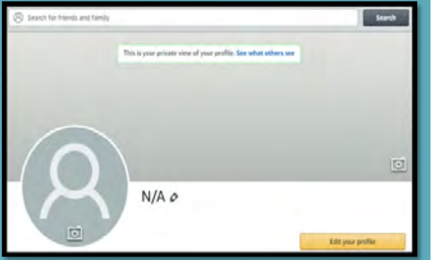
Login with Amazon allows you to log in to registered third-party websites or apps using your Amazon user name and password. It also allows you to opt-in to sharing certain information from your personal profile with the third-party website or app. Additionally, it allows you to provide consent to third-party websites and apps to access and modify data from other Amazon services. Learn More

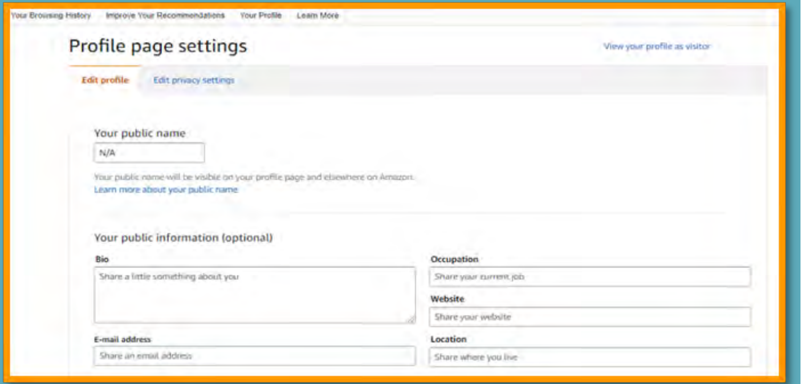
Napster
by Rhapsody Music

You consented on:
September 4, 2017

This connection allows access to:
- Updates you make to the following profile info.
  - Name [redacted]
  - Email address [redacted]@gmail.com

Remove


Search for friends and family
Search
This is your private view of your profile. See what others see
N/A
Edit your profile


Your Browsing History   Improve Your Recommendations   Your Profile   Learn More

Profile page settings   View your profile as visitor

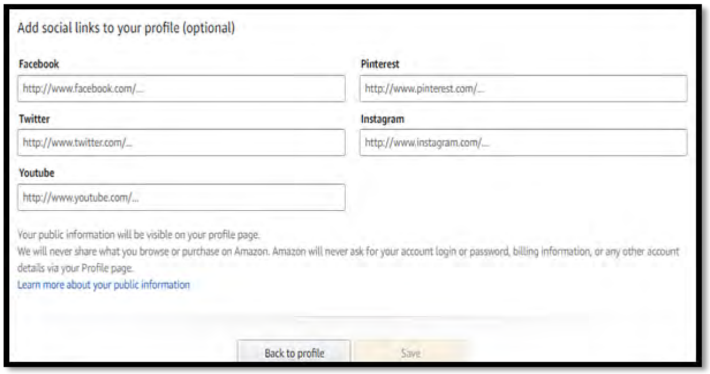
Edit profile   Edit privacy settings

Your public name
N/A
Your public name will be visible on your profile page and elsewhere on Amazon.
Learn more about your public name

Your public information (optional)

Bio: Share a little something about you
Occupation: Share your current job
Website: Share your website
E-mail address: Share an email address
Location: Share where you live

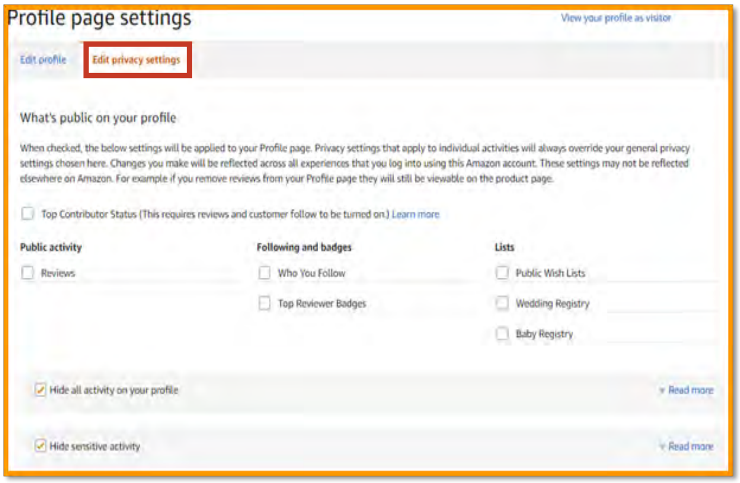
What is Amazon Drive? Amazon Drive is a secure online storage service for your photos, videos and files. Every Amazon customer gets 5 GB of free storage to save, organize, share and access all your files on desktop, mobile and tablet.



Add social links to your profile (optional)

Facebook: http://www.facebook.com/...
Pinterest: http://www.pinterest.com/...
Twitter: http://www.twitter.com/...
Instagram: http://www.instagram.com/...
Youtube: http://www.youtube.com/...

Your public information will be visible on your profile page.
We will never share what you browse or purchase on Amazon. Amazon will never ask for your account login or password, billing information, or any other account details via your Profile page.
Learn more about your public information



Profile page settings

What's public on your profile

When checked, the below settings will be applied to your Profile page. Privacy settings that apply to individual activities will always override your general privacy settings chosen here. Changes you make will be reflected across all experiences that you log into using this Amazon account. These settings may not be reflected elsewhere on Amazon. For example if you remove reviews from your Profile page they will still be viewable on the product page.

□ Top Contributor Status (This requires reviews and customer follow to be turned on.) Learn more

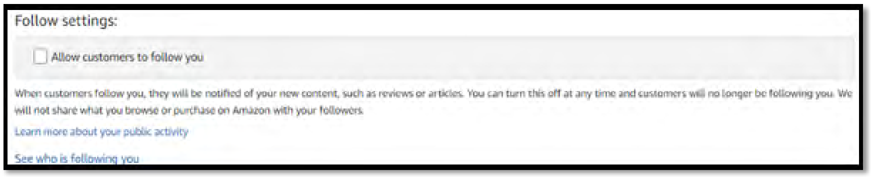
Public activity
□ Reviews

Following and badges
□ Who You Follow
□ Top Reviewer Badges

Lists
□ Public Wish Lists
□ Wedding Registry
□ Baby Registry

☑ Hide all activity on your profile

☑ Hide sensitive activity



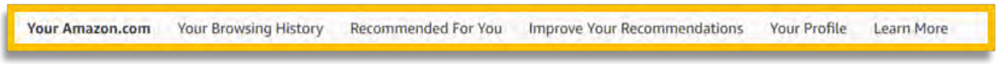
Follow settings:

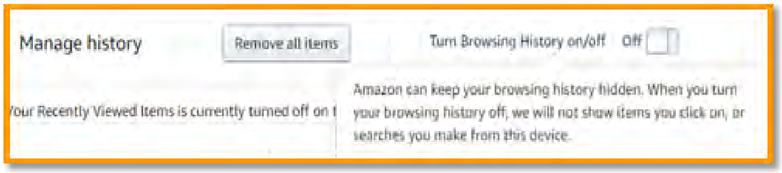
□ Allow customers to follow you

When customers follow you, they will be notified of your new content, such as reviews or articles. You can turn this off at any time and customers will no longer be following you. We will not share what you browse or purchase on Amazon with your followers.

Now let's go to the "Edit privacy settings" to review and make sure they are set. Select "Edit privacy settings" (see above) to review how they are presently configured. We recommend that you select the box "Hide all activity on your profile" as well as "Hide sensitive activity." Users can view their "Profile" as a visitor, by selecting "View your profile as visitor" from the top right of the "Profile page settings." This capability allows users to ensure their profile is properly locked down so that information specific to the User is not readily available to anyone. Next, scroll down to the bottom of the "Edit privacy settings" and make sure the box titled "Allow customers to follow you" is not checked. It is also important to click on the "See who is following you" link to make sure you have not allowed anyone to follow you up to this point .

If you have any followers, you can delete them from this link and then update your privacy settings as shown above to preclude any future followers. We recommend you do not let people follow you on Amazon, but especially if you do not know them.





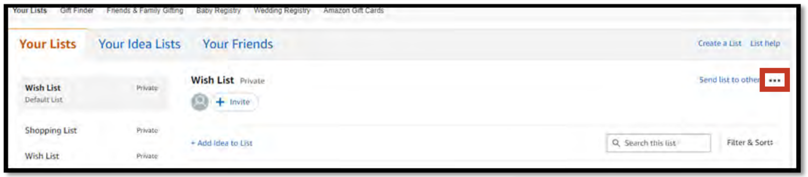
Manage history

Turn Browsing History on/off: Off

Your Recently Viewed Items is currently turned off on t

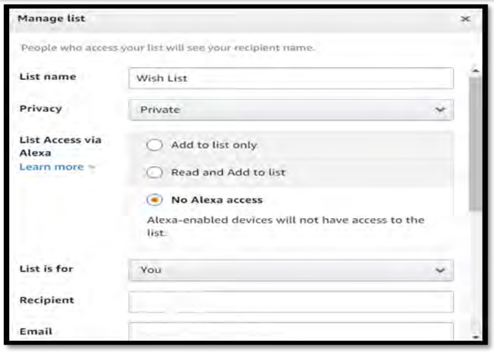
Amazon can keep your browsing history hidden. When you turn your browsing history off, we will not show items you click on, or searches you make from this device.

Now let's take a look at "Your Browsing History". Go to the top menu bar, from either the "Your Profile" section or the "Your followers" page and select "Your Browsing History". From here, look at the right side of your screen and select the drop-down arrow next to "Manage history." From here, it is recommended you remove all items and "Turn Browsing History" to "Off."



Wish List — Private
Default List
Shopping List — Private
Wish List — Private

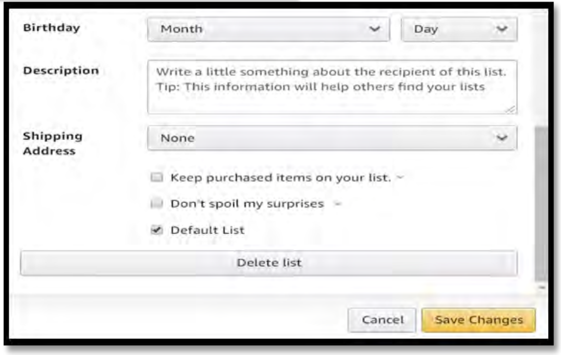
Wish List Private



Manage list

People who access your list will see your recipient name.

List name: Wish List
Privacy: Private
List Access via Alexa
○ Add to list only
○ Read and Add to list
● No Alexa access
Alexa-enabled devices will not have access to the list.
List is for: You
Recipient:
Email:



Birthday: Month / Day
Description: Write a little something about the recipient of this list. Tip: This information will help others find your lists
Shipping Address: None
□ Keep purchased items on your list.
□ Don't spoil my surprises
☑ Default List

One of the most public sections of Amazon is the "Wish Lists." If not made private, anyone can view your lists and gain information about who you are or who the people in your family are (how many, gender, age, etc.). People use "Lists" for making Christmas lists, birthday lists, or even grocery lists. The titles of these lists are revealing (i.e., a child's name for a birthday or Christmas list). These small tid-bits of information could be useful to a social engineer or identity thief when combined with other bits of data on you. Amazon has recently changed its privacy options for "Wish Lists", requiring users to enter an email address in order to access any "Wish List", so make sure that information is locked down. New to the "Wish List", is the option to provide Alexa with access to your "Lists". We do not recommend you provide such access but instead set each list to "Private".

Always remember that a Registry can be created and set for certain times but Amazon will not delete any registry after the "due" date has been reached. It is important for users to go back in and remove/delete any registry themselves after it is no longer needed.

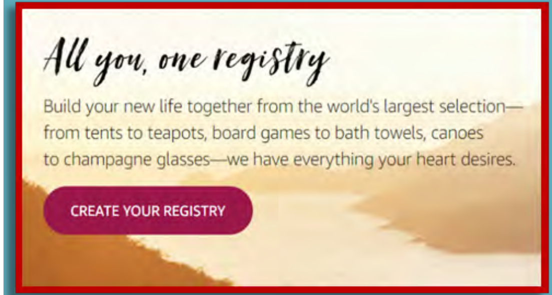
AMAZON SMARTCARD

Select "Manage your list" from "Ordering and Shopping Preferences" in order to begin the process of locking down your lists. Once there, your "Wish Lists" will be on the left-hand side of the screen (see above). In order to review and change these settings, select the ellipse (as shown above in red), and select "Manage List." From there, select "Privacy" and select "Private" from the list. Be sure to select "Save Changes."

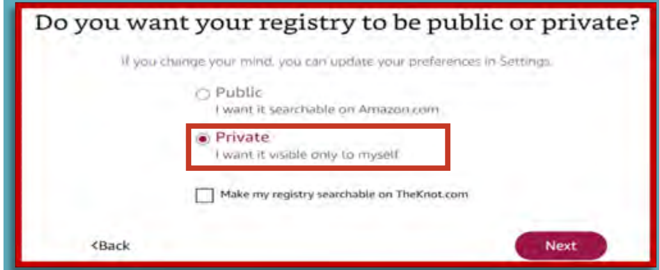
Much like a "Wish List", your registries can also be displayed publicly unless, it is therefore important that you go through the "Settings" for any registry you may build on Amazon. While still in your "Wish List", go to the top menu and select a Registry to create. To create your "Registry" select "Create a new Registry" from the center of your page. Scroll down to "Who can see your registry" and select "Shared" or "Private" for the visibility of your registry. It is important to note that if you decide to make your registry "Public", it may be shared on a third-party website – TheBump or TheKnott - unless you "Unselect" that option. Amazon has created a new registry for birthdays which has many of the same lock down features as the Wedding and Baby registries. Once you have completed the registry and time has passed for its use, it is recommended that you go in remove the data and delete the registry from Amazon.

Head back to the "Account" section and select "Audible Settings" from the second section. Note: this section is only for users who have also signed up and use Audible. In the "Audible Settings" review each section but pay special attention to the "Profile & Preferences" section. Here users will want to ensure that the "Allow other Audible members to see my hoisted location on the Audible" is toggled to the "off" position. At the bottom off this page you can also review what devices are registered and authorized to use your Audible account. If you notice any device that you do not recognize simply select "Deregister" next to that devices name.

Let's take a look at the "Parental Controls" and settings located in the "Video" section of Amazon. To do that you will need to go back to "Your Account" and select "Prime Video Settings" under "Digital content and devices." At the top of the page select "Parental Controls". For parents, it is always important to monitor and protect our children from age-inappropriate material on the internet and television screen. Amazon allows parents to set "Prime Video PINs" and "Viewing Restrictions". Setting the restrictions means that any time someone attempts to play


All you, one registry

Build your new life together from the world's largest selection—from tents to teapots, board games to bath towels, canoes to champagne glasses—we have everything your heart desires.

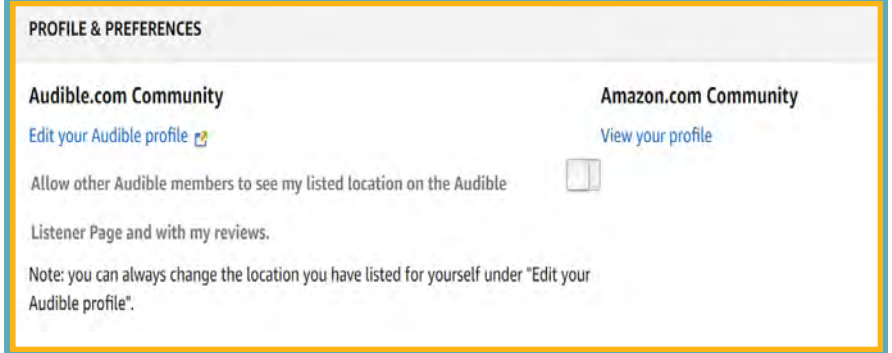

Do you want your registry to be public or private?

If you change your mind, you can update your preferences in Settings.

○ Public
I want it searchable on Amazon.com

● Private
I want it visible only to myself

□ Make my registry searchable on TheKnot.com


PROFILE & PREFERENCES

Audible.com Community

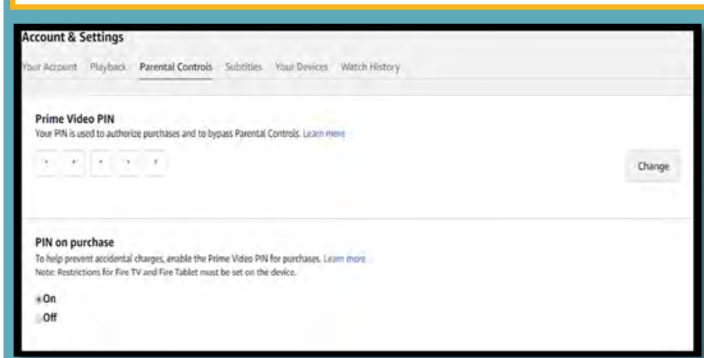
Edit your Audible profile

Allow other Audible members to see my listed location on the Audible Listener Page and with my reviews.

Note: you can always change the location you have listed for yourself under "Edit your Audible profile".

Amazon.com Community

View your profile


Account & Settings

Prime Video PIN

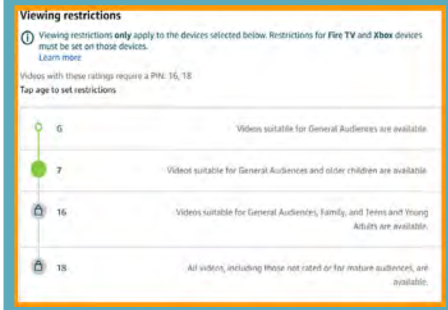
Your PIN is used to authorize purchases and to bypass Parental Controls. Learn more

PIN on purchase

To help prevent accidental charges, enable the Prime Video PIN for purchases. Learn more

Note: Restrictions for Fire TV and Fire Tablet must be set on the device.

● On
○ Off


Viewing restrictions

Viewing restrictions **only** apply to the devices selected below. Restrictions for **Fire TV** and **Xbox** devices must be set on those devices.
Learn more

Videos with these ratings require a PIN: 16, 18

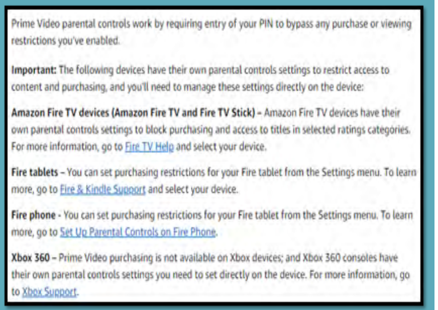
Tap age to set restrictions

6 Videos suitable for General Audiences are available.

7 Videos suitable for General Audiences and older children are available.

16 Videos suitable for General Audiences, Family, and Teens and Young Adults are available.

18 All videos, including those not rated or for mature audiences, are available.


Prime Video parental controls work by requiring entry of your PIN to bypass any purchase or viewing restrictions you've enabled.

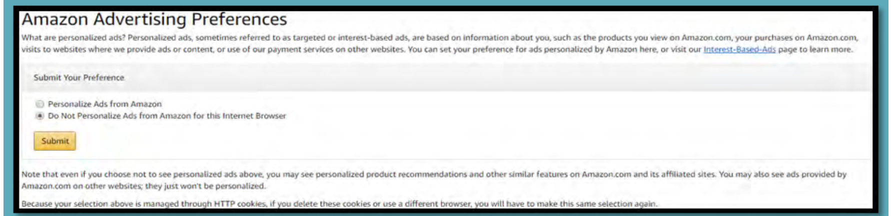
Important: The following devices have their own parental controls settings to restrict access to content and purchasing, and you'll need to manage these settings directly on the device:

Amazon Fire TV devices (Amazon Fire TV and Fire TV Stick) – Amazon Fire TV devices have their own parental controls settings to block purchasing and access to titles in selected ratings categories. For more information, go to Fire TV Help and select your device.

Fire tablets – You can set purchasing restrictions for your Fire tablet from the Settings menu. To learn more, go to Fire & Kindle Support and select your device.

Fire phone - You can set purchasing restrictions for your Fire tablet from the Settings menu. To learn more, go to Set Up Parental Controls on Fire Phone.

Xbox 360 – Prime Video purchasing is not available on Xbox devices; and Xbox 360 consoles have their own parental controls settings you need to set directly on the device. For more information, go to Xbox Support.


Amazon Advertising Preferences

What are personalized ads? Personalized ads, sometimes referred to as targeted or interest-based ads, are based on information about you, such as the products you view on Amazon.com, your purchases on Amazon.com, visits to websites where we provide ads or content, or use of our payment services on other websites. You can set your preference for ads personalized by Amazon here, or visit our Interest-Based-Ads page to learn more.

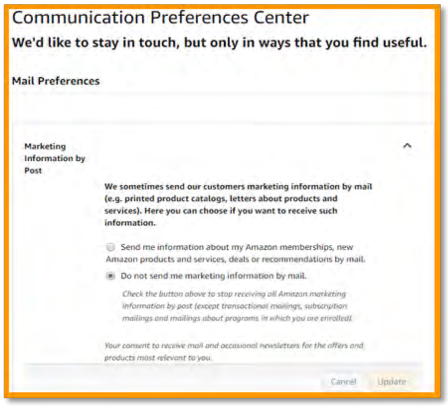
Submit Your Preference

○ Personalize Ads from Amazon
● Do Not Personalize Ads from Amazon for this Internet Browser

Note that even if you choose not to see personalized ads above, you may see personalized product recommendations and other similar features on Amazon.com and its affiliated sites. You may also see ads provided by Amazon.com on other websites; they just won't be personalized.

Because your selection above is managed through HTTP cookies, if you delete these cookies or use a different browser, you will have to make this same selection again.

"Ships from" and "sold by" Amazon.com: This is the real deal and almost certainly not a scam of any kind. Choose this option whenever possible. #themoreyouknow #beatidentitytheft



Communication Preferences Center

We'd like to stay in touch, but only in ways that you find useful.

Mail Preferences

Marketing Information by Post

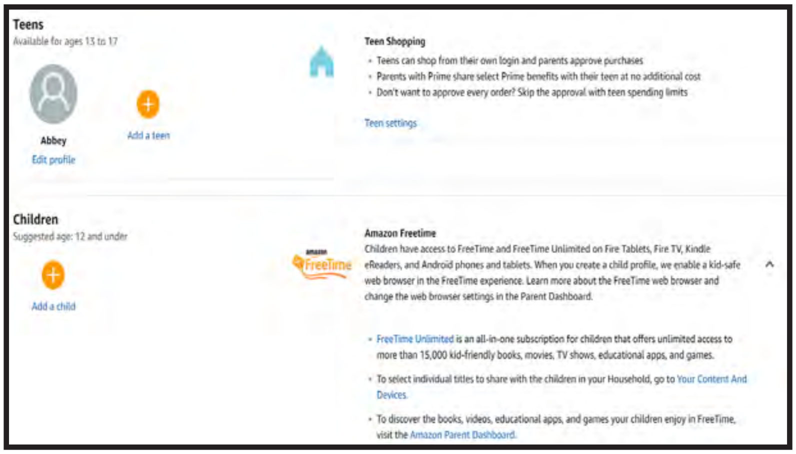
We sometimes send our customers marketing information by mail (e.g. printed product catalogs, letters about products and services). Here you can choose if you want to receive such information.

○ Send me information about my Amazon memberships, new Amazon products and services, deals or recommendations by mail.

● Do not send me marketing information by mail.

Check the button above to stop receiving all Amazon marketing information by post (except transactional mailings, subscription mailings and mailings about programs in which you are enrolled).

Your consent to receive mail and occasional newsletters for the offers and products most relevant to you.



Teens

Available for ages 13 to 17

Teen Shopping

- Teens can shop from their own login and parents approve purchases
- Parents with Prime share select Prime benefits with their teen at no additional cost
- Don't want to approve every order? Skip the approval with teen spending limits

Children

Suggested age: 12 and under

Amazon Freetime

Children have access to FreeTime and FreeTime Unlimited on Fire Tablets, Fire TV, Kindle eReaders, and Android phones and tablets. When you create a child profile, we enable a kid-safe web browser in the FreeTime experience. Learn more about the FreeTime web browser and change the web browser settings in the Parent Dashboard.

- FreeTime Unlimited is an all-in-one subscription for children that offers unlimited access to more than 15,000 kid-friendly books, movies, TV shows, educational apps, and games.
- To select individual titles to share with the children in your Household, go to Your Content And Devices.
- To discover the books, videos, educational apps, and games your children enjoy in FreeTime, visit the Amazon Parent Dashboard.

a video or other content (depending on the device, i.e., the Amazon Fire Stick) they will be required to put in a PIN, which will be designated here by you.

If you scroll down on the "Video Settings" page, you will find the "Viewing Restrictions" section. Here you can select at what age rating you would like a PIN to be required. If you scroll even further down, Amazon lists other Amazon devices (as shown below) that require parental controls be set separately. These settings are inherent to, and accessed from, the devices themselves.

Now let's check the security and privacy settings regarding advertising and communications on your account. Go back to "Your Account" and in the "Communication and Content" section, select "Advertising Preferences" so we can review what Amazon provides to you and to advertisers. Personalized ads, sometimes referred to as targeted or interest-based ads are based on information about you, such as the products you view, the purchases you make on Amazon, or websites you visit where Amazon might provide ads or content.

We recommend you select "Do Not Personalize Ads from Amazon for this Internet Browser." This does exactly what it says in the title, but for the current browser only. Amazon has been known to reset your privacy and other settings if it is opened from a browser different from the one used to lock it down originally. It will also reset your settings if you clear your cookies and delete your internet history. This means that you will need to go back into Amazon and make sure your settings are still intact any time you delete cookies or clear your browser history.

Now let's go back to "Your Account" and select "Communication Preferences." Select the down arrow to the right of "Marketing Information by Post" and select "Do not send me marketing information by mail" (highlighted in red to the right). This will help to eliminate spam and other marketing emails from cluttering your inbox. Be sure to select the "Update" button to save these changes.

Finally, Amazon has different profiles to help you manage your account and any account you may want to create for your children. For instance, a teenager can have their own log in and purchase ability, while parents maintain control over purchases. Parents can also add any children under 12 to their accounts to help manage the content displayed on certain devices, such as the Fire TV. In order to create these accounts or manage these accounts select "Amazon Household" or "Teens Program" from the third and final section under "Account."

"Ships from" and "sold by" [seller]: Third-party seller that ships an item from them directly to you. Amazon doesn't touch the item. This is where scammers thrive. "Sold by" [seller] and "Fulfilled by" Amazon: A third-party seller sends the product to Amazon's warehouse, then Amazon ships . These items can be "Prime" eligible, but are still third-party.

UPDATED JAN 2021

LOCKING DOWN Pinterest

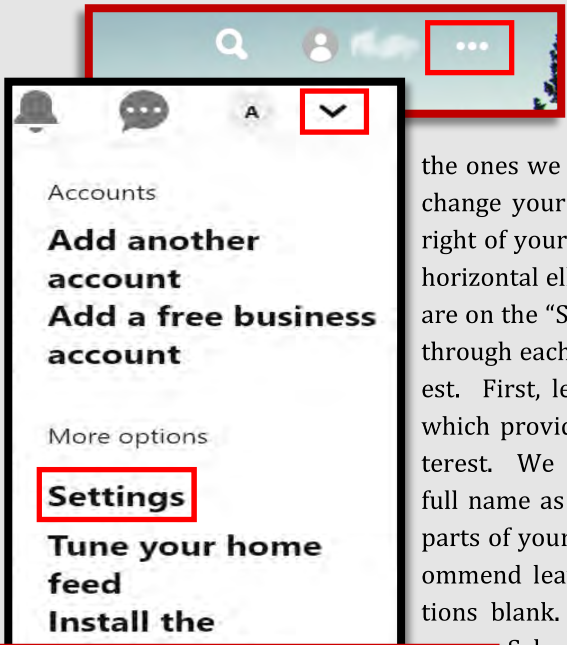
Personal Computer (PC) Version

Do's and Don'ts

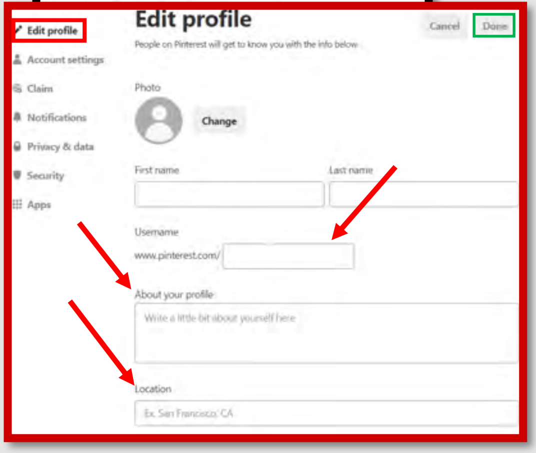
- ***Do*** use Two-Factor Authentication to protect all your information. Like all social media accounts, it is important to make sure your Pinterest is as secured as possible. Two-Factor Authentication is one of the best ways to control your information.
- ***Do*** make sure your email is up to date! If Pinterest suspects nefarious activity on your Pinterest account, they will lock your account down and send your new password to the email address on file.
- ***Do*** monitor what your children and teenagers are looking at on Pinterest. Pinterest does have inappropriate content that, if not specifically tagged as such, will not be flagged or removed by Pinterest.
- ***Do*** make your boards private once you create them so that they are not searchable by any and all Pinners.
- ***Don't*** put personal information on the title of your Pinterest boards. A lot of information can be obtained simply by reading a title (whether or not you have children, rent or own a home, marital status, etc.).

Check your credit report at least once a year. You may also want to check your credit report if you feel any of your social media accounts have been compromised. #beatidentitytheft

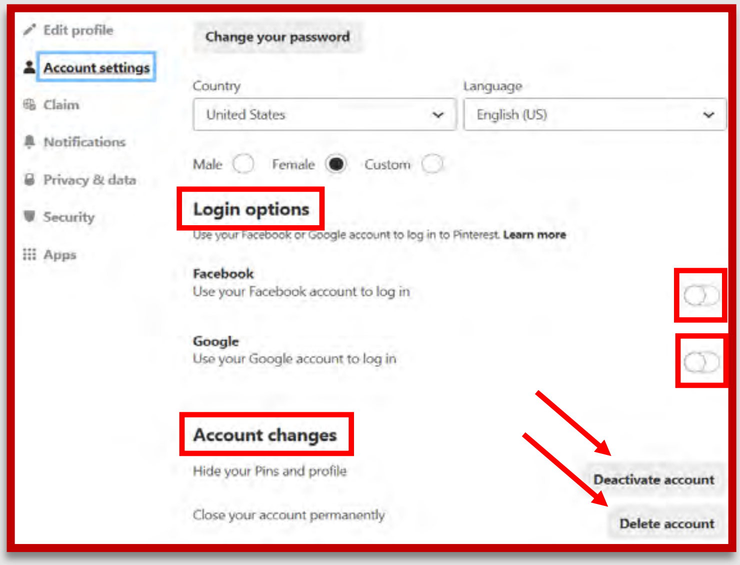
Edit Profile & Account Settings



Since there aren't many privacy settings to manage on Pinterest, it is especially important to ensure the ones we have are locked down. In order to change your Pinterest settings look to the top right of your screen and select "Settings" (three horizontal ellipses, or a down arrow). Once you are on the "Settings" page you will be able to go through each of the settings provided by Pinterest. First, let's review the "Edit Profile" page, which provides your basic information on Pinterest. We recommend you avoid using your full name as your "Username", and instead use parts of your name or a nickname. We also recommend leaving the "Bio" and "Location" sections blank. This information is not required. Select "Done" if you make any changes.



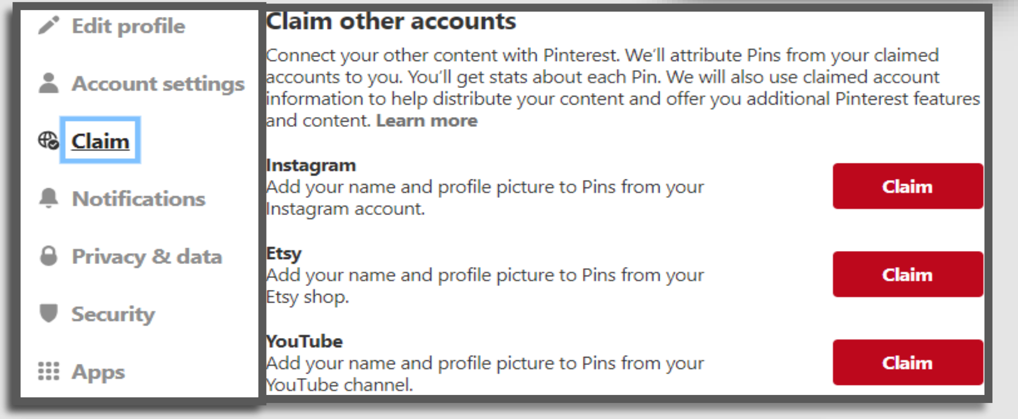
Next, let's review your "Account settings". Under "Account settings" you will find options to change your email address and password, set your login options, and delete or deactivate your account in the case you decide you no longer want to use Pinterest. We recommend you always log in with a unique password used only for Pinterest, and never login via Facebook or Google. Ensure the toggles next to these options are set to "Off". If you decide to deactivate your account for a period of time or delete it altogether, follow the prompts after selecting the correct option. Select "Done" at the top to save your changes.



UPDATED JAN 2021

LOCKING DOWN Pinterest

Personal Computer (PC) Version



- Edit profile
- Account settings
- Claim
- Notifications
- Privacy & data
- Security
- Apps

Claim other accounts

Connect your other content with Pinterest. We'll attribute Pins from your claimed accounts to you. You'll get stats about each Pin. We will also use claimed account information to help distribute your content and offer you additional Pinterest features and content. **Learn more**

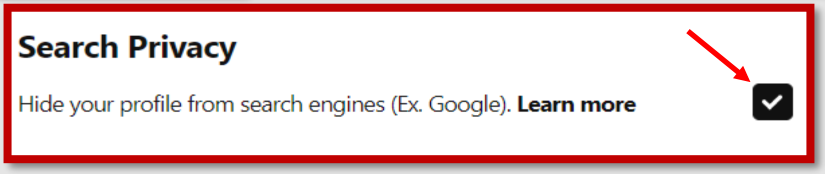
Instagram
Add your name and profile picture to Pins from your Instagram account. **Claim**

Etsy
Add your name and profile picture to Pins from your Etsy shop. **Claim**

YouTube
Add your name and profile picture to Pins from your YouTube channel. **Claim**

Privacy & Security

The next few settings have to do with linking your other social media accounts to Pinterest. **As always, we recommend that you do not link any other social media accounts to Pinterest.** If someone gains access to one of your social media accounts, keeping them separate prevents an intruder from accessing all your other accounts.

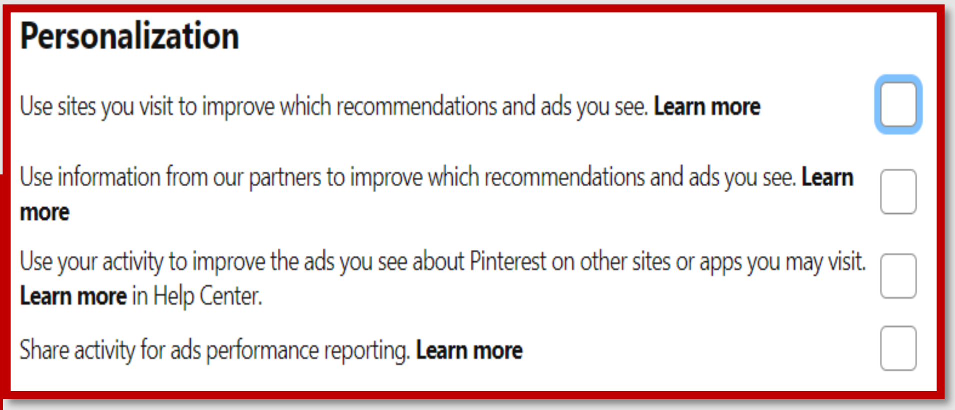


Search Privacy

Hide your profile from search engines (Ex. Google). **Learn more** ☑

First, see the “Claim” section. This option allows you to connect Instagram, Etsy, or YouTube accounts, with the purpose of gaining more popularity for your posts across all platforms. We recommend ***not*** claiming these accounts.

Next, continue down the screen to find “Privacy & data” and review the settings. First, you will see “@Mentions” which allows other Pinterest users to mention you in their comments and pins. It is recommended were feasible that this function be turned off or that “Only people you follow” be allowed to mention your name. Next you will see “Search Privacy”, which left unchecked, will allow your account to be searchable on Google. We recommend you make your account private by checking the box next to “Search Privacy”, as indicated above. Next look at “Personalization” and see the list beneath it. The purposes of these settings are for Pinterest to collect information about you in order to personalize ads and other content for you. We recommend leaving all boxes in this section “Unchecked”. Scrolling to the bottom it is important to review the “Cookie Preferences” to ensure you have not allowed any unnecessary cookies to be collected.



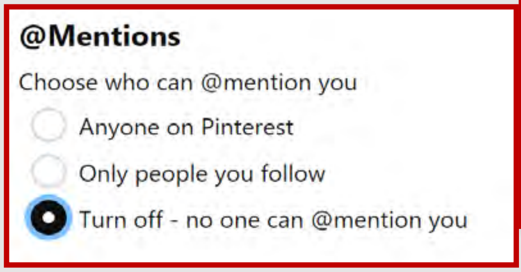
Personalization

Use sites you visit to improve which recommendations and ads you see. **Learn more** ☐

Use information from our partners to improve which recommendations and ads you see. **Learn more** ☐

Use your activity to improve the ads you see about Pinterest on other sites or apps you may visit. **Learn more** in Help Center. ☐

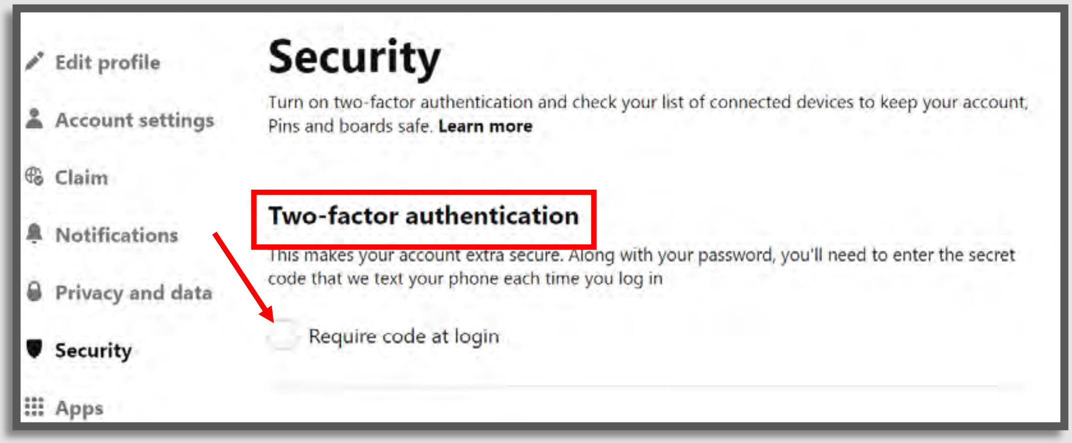
Share activity for ads performance reporting. **Learn more** ☐



@Mentions

Choose who can @mention you

○ Anyone on Pinterest
○ Only people you follow
● Turn off - no one can @mention you



- Edit profile
- Account settings
- Claim
- Notifications
- Privacy and data
- Security
- Apps

Security

Turn on two-factor authentication and check your list of connected devices to keep your account, Pins and boards safe. **Learn more**

Two-factor authentication

This makes your account extra secure. Along with your password, you'll need to enter the secret code that we text your phone each time you log in

☐ Require code at login

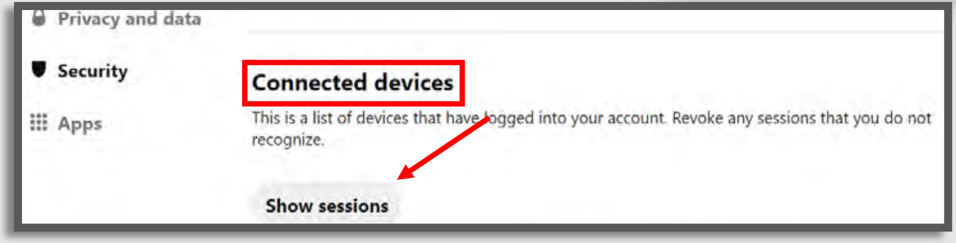
Now let’s visit the “Security” section, which allows you options for better account security. The first section is for “Two-factor Authentication”, which we strongly recommend you enable. Select the box next to “Require code at login”, and you will have the option of having a code sent to your mobile device that you will need to enter when you log in - a new code will be sent each time you log in. This is the highest level of security you can

Make sure your antivirus and antimalware software stays up to date. Keeping software up to date helps to prevent advanced malware and viruses from affecting your computer.

UPDATED JAN 2021

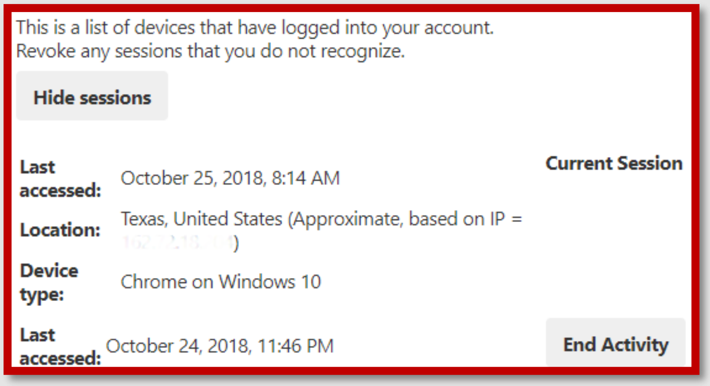
LOCKING DOWN Pinterest

Personal Computer (PC) Version



Connected devices

This is a list of devices that have logged into your account. Revoke any sessions that you do not recognize.



This is a list of devices that have logged into your account. Revoke any sessions that you do not recognize.

Last accessed: October 25, 2018, 8:14 AM

Location: Texas, United States (Approximate, based on IP = [redacted])

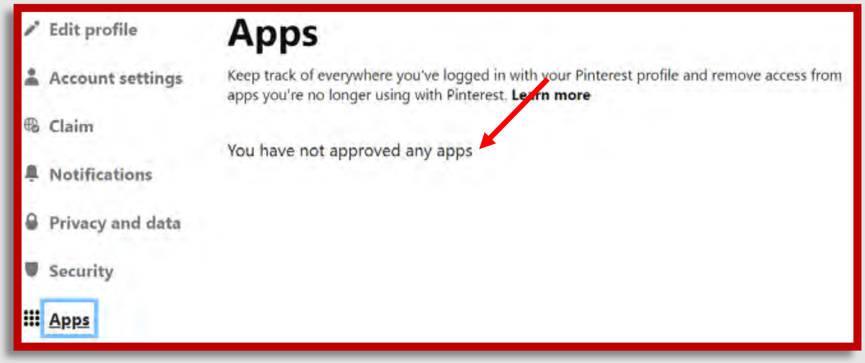
Device type: Chrome on Windows 10

Last accessed: October 24, 2018, 11:46 PM

Privacy & Security, ctd.

Under "Two-factor Authentication", you will see "Connected devices". Select "Show sessions" in this section and you will be provided the opportunity to "End Activity" for all sessions that may seem suspicious or are not needed. If you suspect that your Pinterest account may have been compromised, the "Show Sessions" section may help you to identify a suspicious account and "End Activity" so that you can secure your account and change your password. It is a good idea to go through the "Show Sessions" section periodically and clean it up.

Remove your last name. A Pinterest profile is always open, everyone can see your profile picture and name. This is a severe privacy issue. For greater privacy, remove your last name and/or change your username (shown in the URL) to be something nonspecific to you. It is also recommended that users use an anonymous profile picture. Also remember ***not*** to link your Pinterest account with any other social media accounts.



Apps

Keep track of everywhere you've logged in with your Pinterest profile and remove access from apps you're no longer using with Pinterest. **Learn more**

You have not approved any apps

Finally, the "Apps" section allows you to disconnect any third-party apps you might have linked to your account. Again, we recommend keeping all accounts separate for the best security. If you were to lose your mobile device or computer, you do not want someone to have full access to all of your accounts, including Pinterest. If there are any apps listed in this section, we recommend deleting them.

Hide your profile from search engines. The default Pinterest settings allow your profile to come up in search results when someone searches your name on a search engine. This gives access to your online activity to anyone who knows your name. Hide your profile by opening the "Settings" > "Privacy and data" > "Hide your profile from search engines".

Remember if a "Pin" seems too good to be true it very likely is. Pinterest has many spam "pins" where a single click can lead to a third party site. #staysafeonline

UPDATED JAN 2021

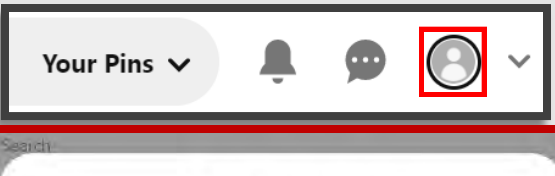
LOCKING DOWN Pinterest

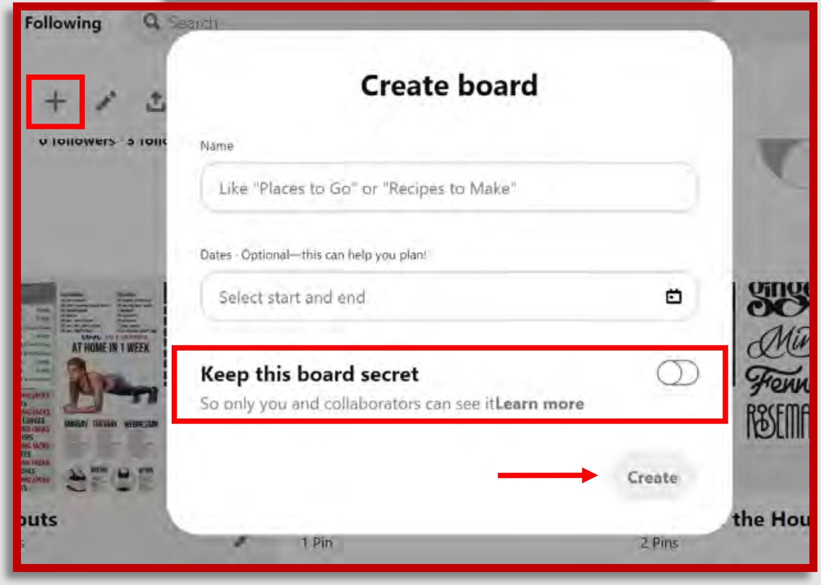
Personal Computer (PC) Version

Visible Content

What you display on your Pinterest account reveals a lot of information about you, so you have to be careful about what you "Pin". Everything that you "Pin" is public. Not just your followers, but everyone can see your profile and what you pin. Pinterest has no means of limiting the visibility of your "Pins" or your "Comments" like there are on other social media platforms (unless you make them "Secret", which is discussed next). Once a "Pin" or "Comment" is loaded, there is no taking it back.

Take a look at the titles of your "Boards", and make sure they reveal no information about you or your family. For instance, do any of them have names of children, schools, churches, workplaces, etc? Also, take a look at your whole collection of "Boards" to see what kind of narrative it tells about you. Consider that all your "Boards" and "Pins" together paint a pretty illuminating picture of your interests, values and lifestyle.





Name

Like "Places to Go" or "Recipes to Make"

Dates · Optional—this can help you plan!

Select start and end

Keep this board secret ○

So only you and collaborators can see itLearn more

There is only one way to ensure full control over your "Boards" and "Pins", which is by setting them to "Secret". When you use this feature, no one can see your content unless you specifically invite them to. We recommend you consider setting some or all of your "Boards" to "Secret" in order to limit the amount of information someone can gather about you.

To create a "Secret Board", select your "Profile Icon" in the top right corner of the page. Then select the "+" icon to create a new "Board", name the board, and set the toggle next to "Keep this board secret" to "On". Select the "Create" button. Only the creator of the "Secret Board" has control over its features, and with whom content is shared. You must invite "Collaborators" via email in order for them to see the content. When you "Pin" content to a "Secret Board", the "Pins" are also private. Only the creator can make the board public, and when you do, all content is made public, including all "Pins" and "Comments". In order to change a "public" board to a "Secret board" simply open the board you wish to change, then select the three dots next to the board title. From the drop down select "Edit board." Scroll down to select "Keep this board secret" then hit "done."

Scam Pins: Keep an eye out for "Scam Pins" that might be advertising "Amazing Weight-loss Techniques" or "Free Gift Cards". These scams lead you to a scam website and ask you to fill out a survey with personal information, download malware, or share the "Pin" forward. To avoid "Scam Pins", you should pay attention to the URL with every single pin. The URL is located at the bottom left of a pin. Avoid any pin that leads to an unofficial or fishy URL.

Everything you post on Pinterest can be seen by the "Public". The ONLY way to maintain full control of your pins is to create a "Secret Board".

UPDATED JAN 2021

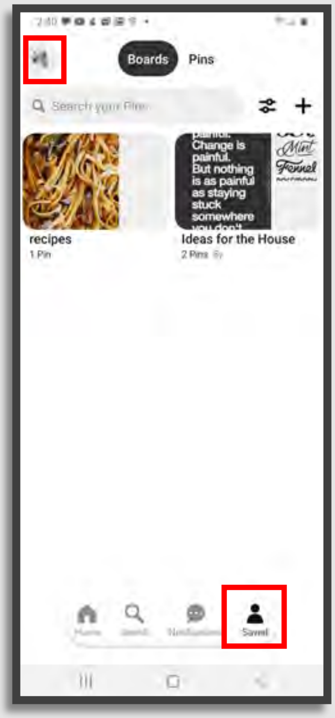
LOCKING DOWN Pinterest

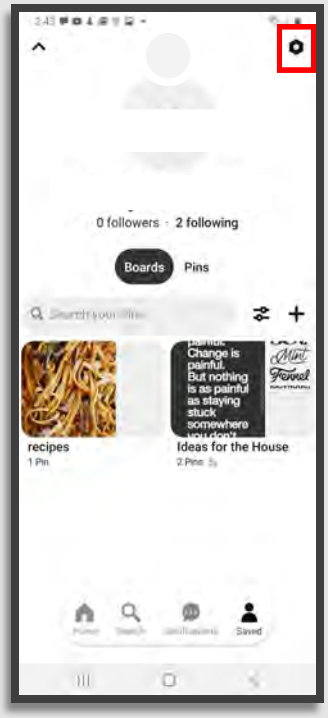
Mobile Device Version

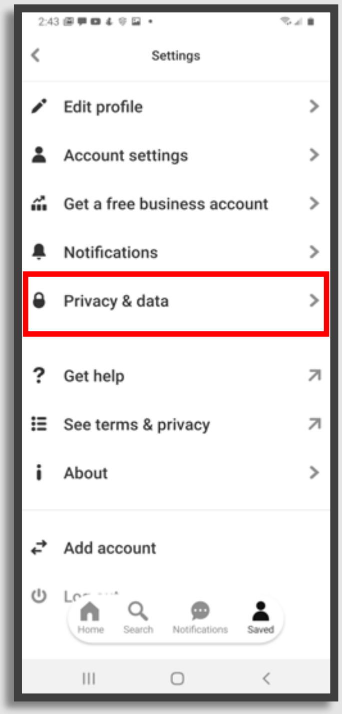
*** This information describes how to make your account secure on Android and iPhone mobile devices. Most images provided are of Android screens. Differences between iPhone Operating System (iOS) and Android Operating System (AOS) are minimal - when they are significant, such differences are noted specifically.*

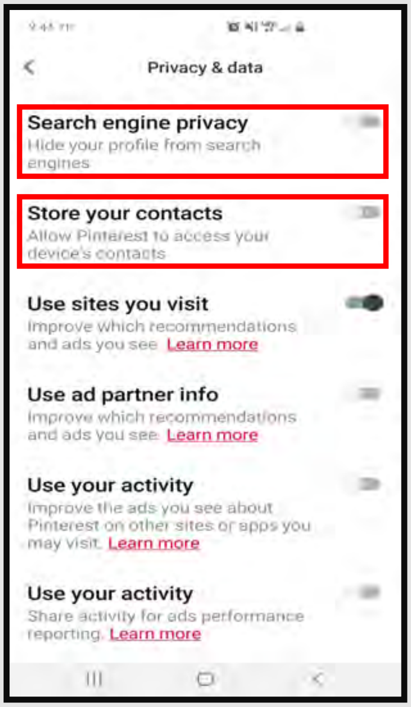
Security & Privacy

On your mobile device, you will begin at your "Profile" screen by selecting the "Profile" icon at the bottom right of the screen, or locating your "Profile Picture" on the page. Then select the "Settings" icon at the top right. The "Edit profile" and "Account settings" are the same as the computer version. However, the "Privacy & data" section is a little different on the mobile version. If you select "Privacy & data", then see "Store your contacts", and ensure the toggle is set to "Off". Additionally, make sure that all your privacy settings are set the way you want them, in case the settings you chose via computer did not transfer to the mobile app.








Privacy & data

Search engine privacy
Hide your profile from search engines

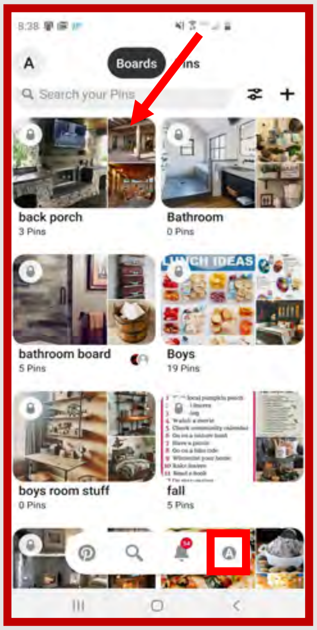
Store your contacts
Allow Pinterest to access your device's contacts

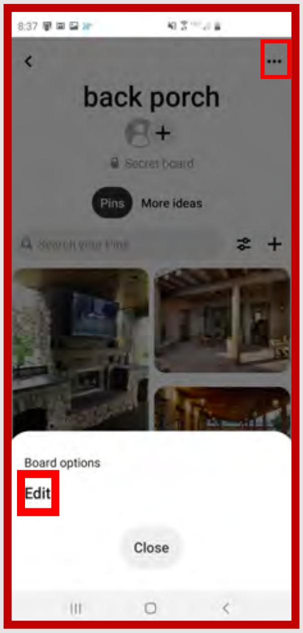
Use sites you visit
Improve which recommendations and ads you see Learn more

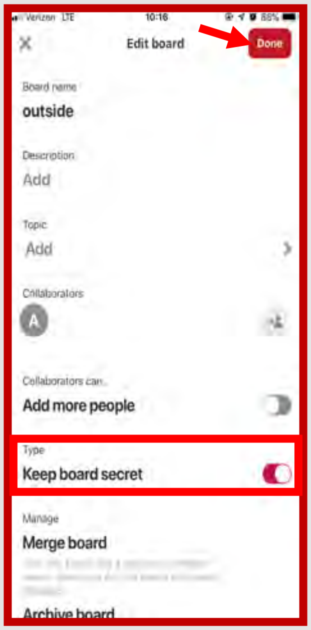
Use ad partner info
Improve which recommendations and ads you see Learn more

Use your activity
Improve the ads you see about Pinterest on other sites or apps you may visit. Learn more

Use your activity
Share activity for ads performance reporting. Learn more






Edit board

Done

Board name
outside

Description
Add

Topic
Add

Collaborators

Collaborators can
Add more people

Type
Keep board secret

Manage
Merge board

Archive board

Visible Content

To make a "Secret Board" on your mobile device, first go to your account by selecting the "Profile" icon at the bottom right of the screen. Select the "Board" you want to make private, then select the "Menu" icon, or ". . . " at the top right of the screen, select "Edit", then scroll down to "Keep board secret", and set the toggle to "On". To save your changes, select the "Done" button at the top right of the screen.

While Pinterest is full of entertaining content, remember it is for all ages and as such its content can be "for Adults Only" and not what you want your children to see.

UPDATED JAN 2021

LOCKING DOWN

Pinterest HACKED

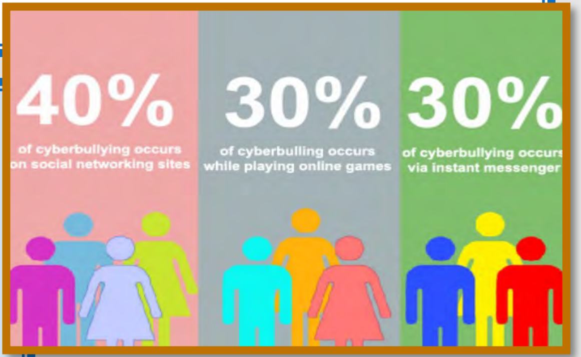
Indicators of Possible Account Compromise:

Do you think your account may have been compromised or hacked? Have you noticed any of the following:

- Unexpected posts posted by your account
- Direct Messages sent from your account that you did not initiate
- Other account behaviors you didn't perform or approve (like following, unfollowing, blocking, etc.)
- A notification from Pinterest stating that your account may be compromised
- A notification from Pinterest stating that your account information (bio, name, etc.) has changed
- Your password is no longer working or you are being prompted to reset it. *If this occurs it is highly recommended that you sign-in online and change your password immediately.

If you said "Yes" to any of the above , it is advised you take the following actions:

- Delete any unwanted pins that were posted while your account was compromised
- Scan your computers for viruses and malware, especially if unauthorized account behaviors continue to be pinned after you've changed your password
- Make sure to change your password. Always use a strong password you haven't used elsewhere and would be difficult to guess
- Consider using login verification (if you haven't done so already), instead of relying on just a password. Login verification introduces a second check to make sure that you and only you can access your Pinterest account
- Be sure to check that your email is secure. It may be worth changing the password to both your Pinterest account and the email associated with your Pinterest account. *If you feel your email may have been compromised and need help finding the right contact information for your email provider please see page 21 of this smart book under the "blue box" at the bottom of the page.



If you need report a pin, comment, or message: https://help.pinterest.com/en/article/report-something-on-pinterest

If your account was hacked: https://help.pinterest.com/en/contact, then go to "Account Access and Closure," "Login Issues, "Continue" and follow the steps to describe your specific situation.

If you find that you or someone else is being bullied or harassed go to: https://help.pinterest.com/en/article/report-harassment-and-cyberbullying

If you cannot log in to your email account, Twitter has provided links to each email account's "having trouble signing in" page for your convenience. https://help.twitter.com/en/managing-your-account/cant-access-my-accounts-email-address

If you still need help or have questions, you can always contact Pinterest by: https://help.pinterest.com/en/contact?page=about_you_page

If you do not have access to the email you originally signed up on Pinterest with or believe it may have been hacked, Pinterest will allow you to provide an alternate email for communication. This can be both good and bad for Users. While it can provide peace of mind if you need to regain access to your account, it does create its own vulnerability and Users should be aware of this.

UPDATED JAN 2021

LOCKING DOWN YOUR SNAPCHAT

Mobile Device Version

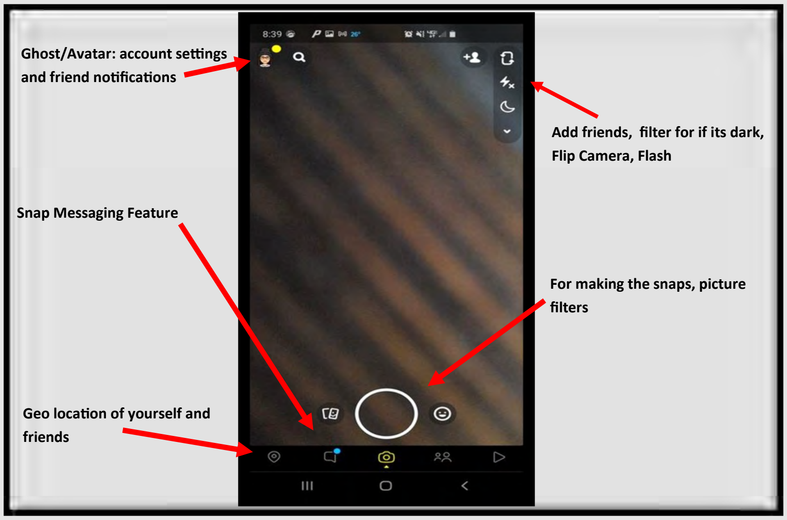
*** This information describes how to make your account secure on Android and iPhone mobile devices. Differences between iPhone Operating System (iOS) and Android Operating System (AOS) are significant for some features, and in these cases iPhone images are outlined* ***black*** *and Android* ***yellow****.*

As of March 2020, there are an estimated 229 million Snapchat users. Make sure you know who your children are talking to. #keepourkidssafe

Do's and Don'ts

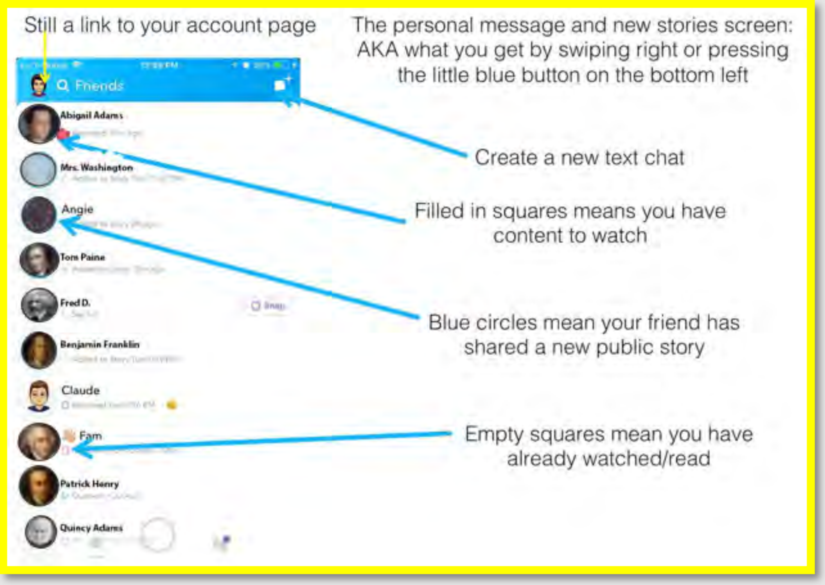
- Do set up privacy and security settings on your Snapchat and help your teenager to do the same.
- Do assume ALL information and images you share are publicly viewable, regardless of your settings.
- Do talk to your teenager about the dangers inherent to Snapchat. Make sure they know to come and tell you if someone they don't know tries to contact them or sends them inappropriate material.
- Do ***not*** add your birthdate, location, or other personal details to online profiles.
- Do ***not*** allow users you do not know personally to contact you via Snapchat.
- Do ***not*** believe that all pictures and videos are automatically deleted. There are ways to save and share content despite Snapchat's efforts to make all communications disappear.

Snapchat is an image and video messaging app that allows users to share multimedia messages that will "self destruct" in up to 10 seconds. It's communication style is meant to mirror real life face-to-face interactions that are temporary, and not stored anywhere. Content is designed to delete automatically, but most users are aware that content can be saved using screen shots or other software.


Ghost/Avatar: account settings and friend notifications
Add friends, filter for if its dark, Flip Camera, Flash
Snap Messaging Feature
For making the snaps, picture filters
Geo location of yourself and friends

The best way to begin understanding and locking down Snapchat's capabilities is to familiarize yourself with Snapchat basics. In the box above you can look over the main icons and functions located in Snapchat. Your "Home Screen" is shown above. You know you are there when you have a "Camera View". One of the main features of the app is making "Snaps", via photos, which you would do from this screen, then share with your "Friends". Next, identify your "Profile" picture at the top left of the box (highlighted in **red**), this icon will take you to your Snapchat statistics and the "Settings" icon.

Shown to the right is an overview of the "Chat" feature of Snapchat. Select the "Chat" icon on the lower left corner of the screen (above in **red**). Here you can see if someone has sent you a message, posted a story, or reviewed your posts. You can also start a "Chat". For now, let's select your "Profile" icon at the top left and head to your Snapchat stats and "Settings" section.


Still a link to your account page
The personal message and new stories screen: AKA what you get by swiping right or pressing the little blue button on the bottom left
Friends
Abigail Adams
Mrs. Washington
Angie
Tom Paine
Fred D.
Benjamin Franklin
Claude
Fam
Patrick Henry
Quincy Adams
Create a new text chat
Filled in squares means you have content to watch
Blue circles mean your friend has shared a new public story
Empty squares mean you have already watched/read

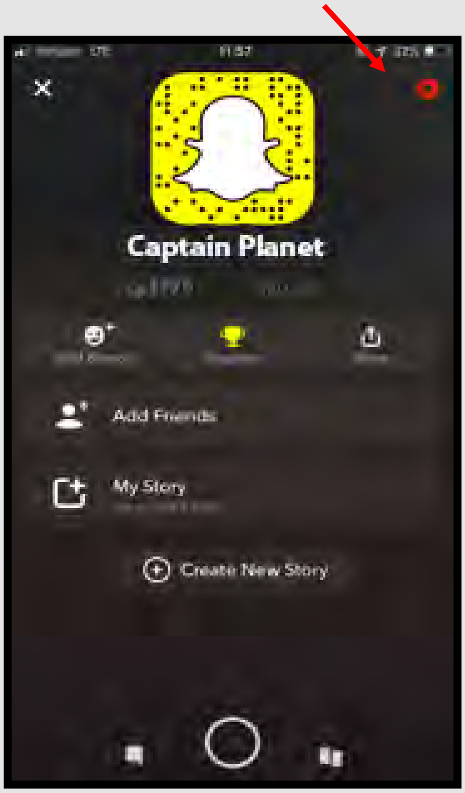
UPDATED JAN 2021

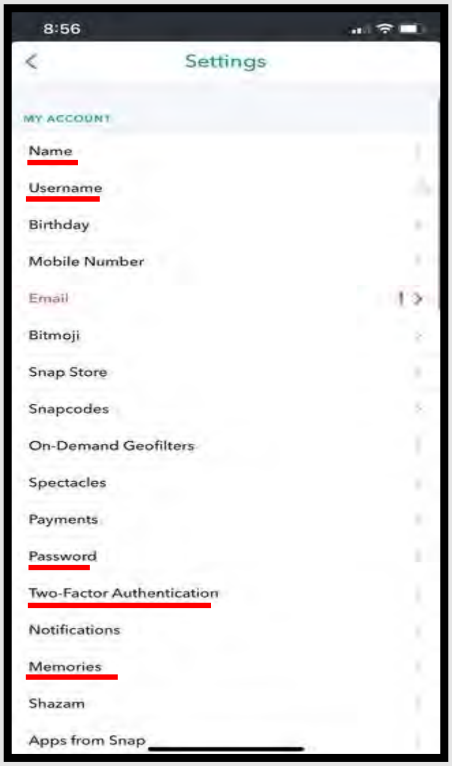
LOCKING DOWN YOUR SNAPCHAT

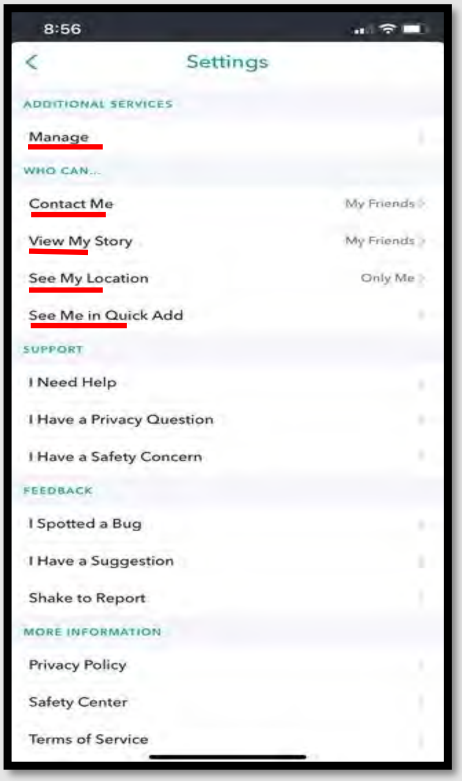
Mobile Device Version

*** This information describes how to make your account secure on Android and iPhone mobile devices. Differences between iPhone Operating System (iOS) and Android Operating System (AOS) are significant for some features, and in these cases iPhone images are outlined* ***black*** *and Android* ***yellow****.*

The Pew Internet and American Life Project found 15% of teenagers ages 12 to 17 acknowledge they received a "sext" from someone they know.







Contact Me: My Friends

View My Story: My Friends

See My Location: Only Me

See Me in Quick Add

After reviewing the different sections on page one of this Card, let us begin locking down your account.

Begin by selecting your "Profile" picture at the top left of the screen on your "Home Page". Next select the "Settings" icon from the top right corner of the screen (shown above in **red**).

From here we can review all of the settings offered by Snapchat:

The "Settings" screens on iPhone and Android have a few differences on Snapchat. Throughout this Card, you will find iPhone screenshots outlined in ***black***, and Android screenshots in *yellow*.

First, check out your "Name" and "Username", and make sure they don't give too much information about you. We recommend you use a nickname or a mixture of names instead of using your full name, and never add birthdays or other significant information to your name. You do not need to put your real birthday on your account, and should consider using an inaccurate one.

Next, we recommend using a "Password" that is unique to Snapchat. As with all of your social media accounts, reusing passwords creates an unnecessary vulnerability, and you should use unique passwords for each account.

On the next page, we will go through the underlined menu items from the above 2 screenshots.

Geo-filters: location-specific elements that can only be unlocked by visiting a specific place. If the Geo-filters are shared, especially by teenagers, any individual could find or track them, to include predators. For all "Locations" It is recommended that this function be set to "Only Me" Additionally, Snapchat will now direct users together more precisely if "location" is turned on, by providing step by step direction.

Snapcash: like PayPal or Venmo, Snapcash lets users transfer money to each other.

Memories: Users can store snaps to appear as memories for later use, however this this is not recommended.

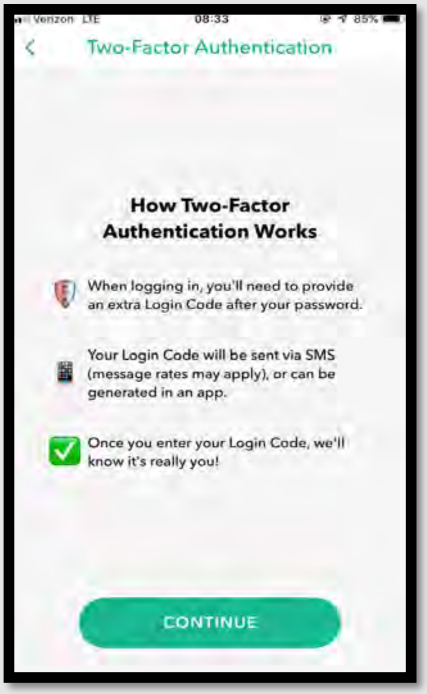
UPDATED JAN 2021

LOCKING DOWN YOUR SNAPCHAT

Mobile Device Version

*** This information describes how to make your account secure on Android and iPhone mobile devices. Differences between iPhone Operating System (iOS) and Android Operating System (AOS) are significant for some features, and in these cases iPhone images are outlined **black** and Android **yellow**.*

Two-Factor Authentication



Verizon LTE 08:33 85%

Two-Factor Authentication

How Two-Factor Authentication Works

When logging in, you'll need to provide an extra Login Code after your password.

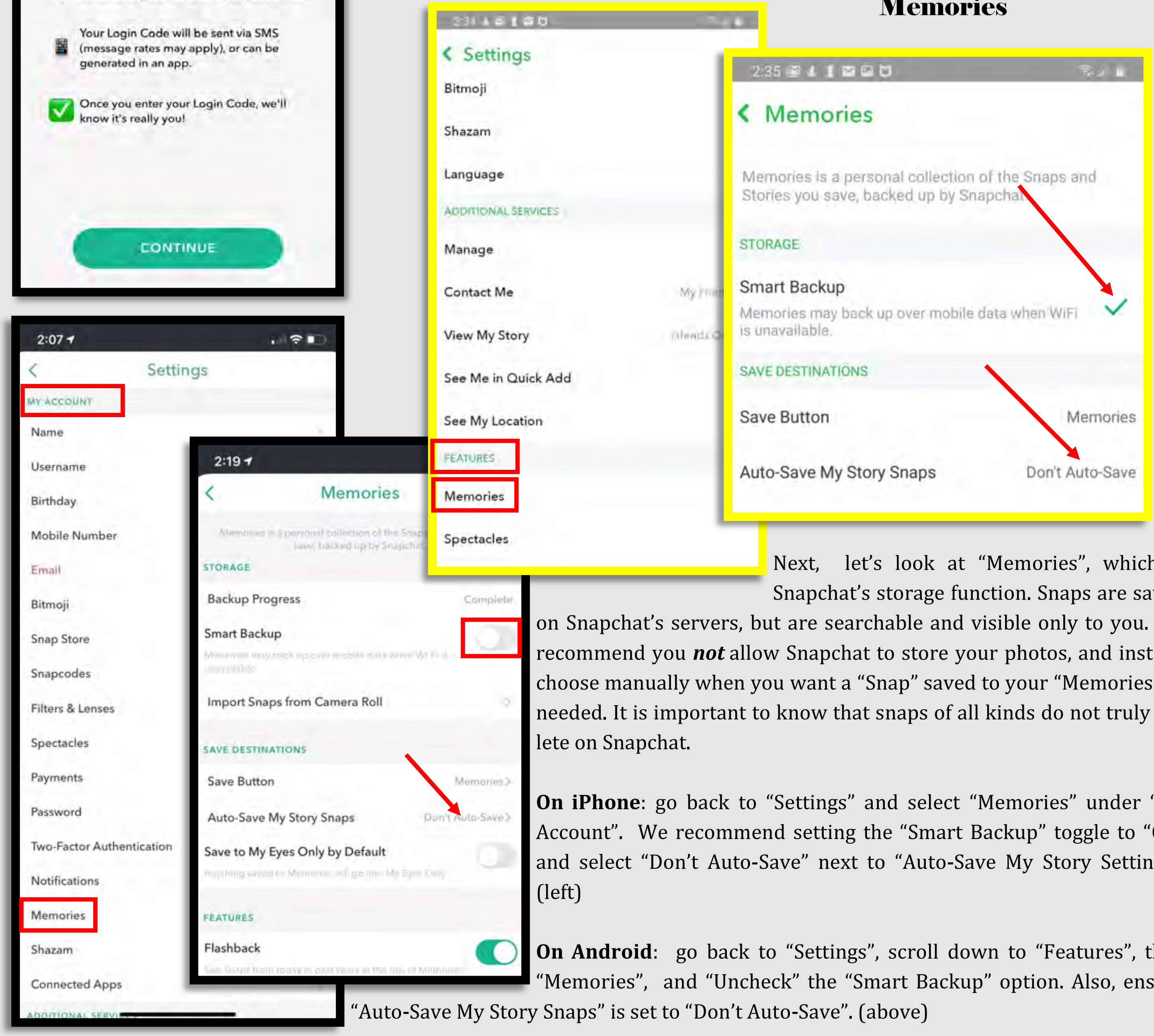
Your Login Code will be sent via SMS (message rates may apply), or can be generated in an app.

✓ Once you enter your Login Code, we'll know it's really you!

CONTINUE

"Two-Factor Authentication" is the most secure option you have for Snapchat security and privacy. To enable it, select "Two-Factor Authentication" from the "Settings" menu, under the first section titled "My Account" (shown on page 2 of this card) and follow the prompts to complete the process. Also referred to as "Login Verification", this feature requires you to enter ***both*** your password and a verification code that is sent to your phone, each time you log in on a new device.

Memories



2:31

Settings

Bitmoji

Shazam

Language

ADDITIONAL SERVICES

Manage

Contact Me — My Frien

View My Story — Friends O

See Me in Quick Add

See My Location

FEATURES

Memories

Spectacles

2:35

Memories

Memories is a personal collection of the Snaps and Stories you save, backed up by Snapchat.

STORAGE

Smart Backup ✓

Memories may back up over mobile data when WiFi is unavailable.

SAVE DESTINATIONS

Save Button — Memories

Auto-Save My Story Snaps — Don't Auto-Save

2:07

Settings

MY ACCOUNT

Name

Username

Birthday

Mobile Number

Email

Bitmoji

Snap Store

Snapcodes

Filters & Lenses

Spectacles

Payments

Password

Two-Factor Authentication

Notifications

Memories

Shazam

Connected Apps

ADDITIONAL SERVICES

2:19

Memories

Memories is a personal collection of the Snaps and Stories you save, backed up by Snapchat.

STORAGE

Backup Progress — Complete

Smart Backup ○

Memories may back up over mobile data when Wi-Fi is unavailable.

Import Snaps from Camera Roll

SAVE DESTINATIONS

Save Button — Memories >

Auto-Save My Story Snaps — Don't Auto-Save >

Save to My Eyes Only by Default ○

Anything saved to Memories will go into My Eyes Only

FEATURES

Flashback ●

See Snaps from today in past years at the top of Memories

Next, let's look at "Memories", which is Snapchat's storage function. Snaps are saved on Snapchat's servers, but are searchable and visible only to you. We recommend you ***not*** allow Snapchat to store your photos, and instead choose manually when you want a "Snap" saved to your "Memories" as needed. It is important to know that snaps of all kinds do not truly delete on Snapchat.

On iPhone: go back to "Settings" and select "Memories" under "My Account". We recommend setting the "Smart Backup" toggle to "Off" and select "Don't Auto-Save" next to "Auto-Save My Story Settings". (left)

On Android: go back to "Settings", scroll down to "Features", then "Memories", and "Uncheck" the "Smart Backup" option. Also, ensure "Auto-Save My Story Snaps" is set to "Don't Auto-Save". (above)

90% of Snapchat users are 13-24 years old, and 69% of U.S. teens say they use Snapchat. Talk to your child about acceptable behavior on Snapchat.

UPDATED JAN 2021

LOCKING DOWN YOUR SNAPCHAT

Mobile Device Version

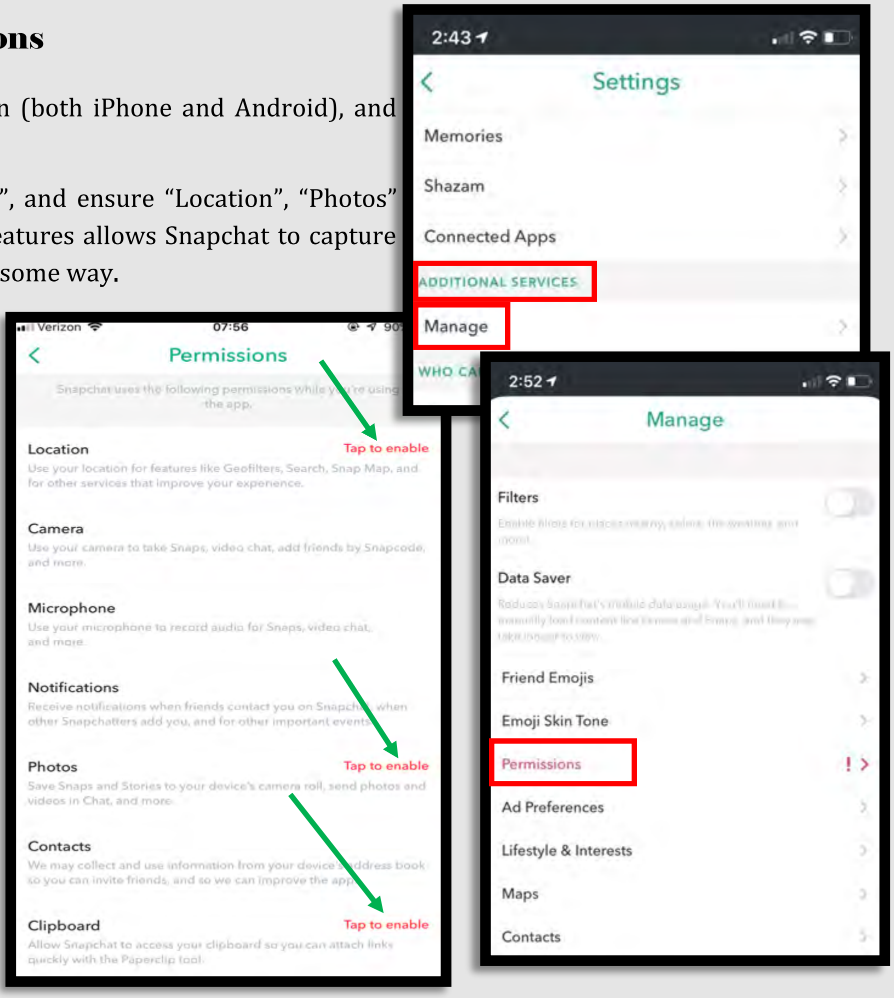
*** This information describes how to make your account secure on Android and iPhone mobile devices. Differences between iPhone Operating System (iOS) and Android Operating System (AOS) are significant for some features, and in these cases iPhone images are outlined **black** and Android **yellow**.*

Hackers have been known to publish thousands of snaps mainly of 13 to 17 year old's. Talk to your teenagers about who they are connecting with.

Manage Permissions

Next, let's go to the "Additional Services" section (both iPhone and Android), and locate the "Manage" option.

On iPhone: select "Manage", then "Permissions", and ensure "Location", "Photos" and "Clipboard" are ***not*** enabled. Each of these features allows Snapchat to capture and store information from your mobile device in some way.



2:43

Settings

Memories

Shazam

Connected Apps

ADDITIONAL SERVICES

Manage

WHO CA

Verizon 07:56

Permissions

Snapchat uses the following permissions while you're using the app.

Location — Tap to enable
Use your location for features like Geofilters, Search, Snap Map, and for other services that improve your experience.

Camera
Use your camera to take Snaps, video chat, add friends by Snapcode, and more.

Microphone
Use your microphone to record audio for Snaps, video chat, and more.

Notifications
Receive notifications when friends contact you on Snapchat, when other Snapchatters add you, and for other important events.

Photos — Tap to enable
Save Snaps and Stories to your device's camera roll, send photos and videos in Chat, and more.

Contacts
We may collect and use information from your device's address book so you can invite friends, and so we can improve the app.

Clipboard — Tap to enable
Allow Snapchat to access your clipboard so you can attach links quickly with the Paperclip tool.

2:52

Manage

Filters
Enable filters for places nearby, unlock the weather and more!

Data Saver
Reduces Snapchat's mobile data usage. You'll need to manually load content like Lenses and Snaps, and they may take longer to view.

Friend Emojis

Emoji Skin Tone

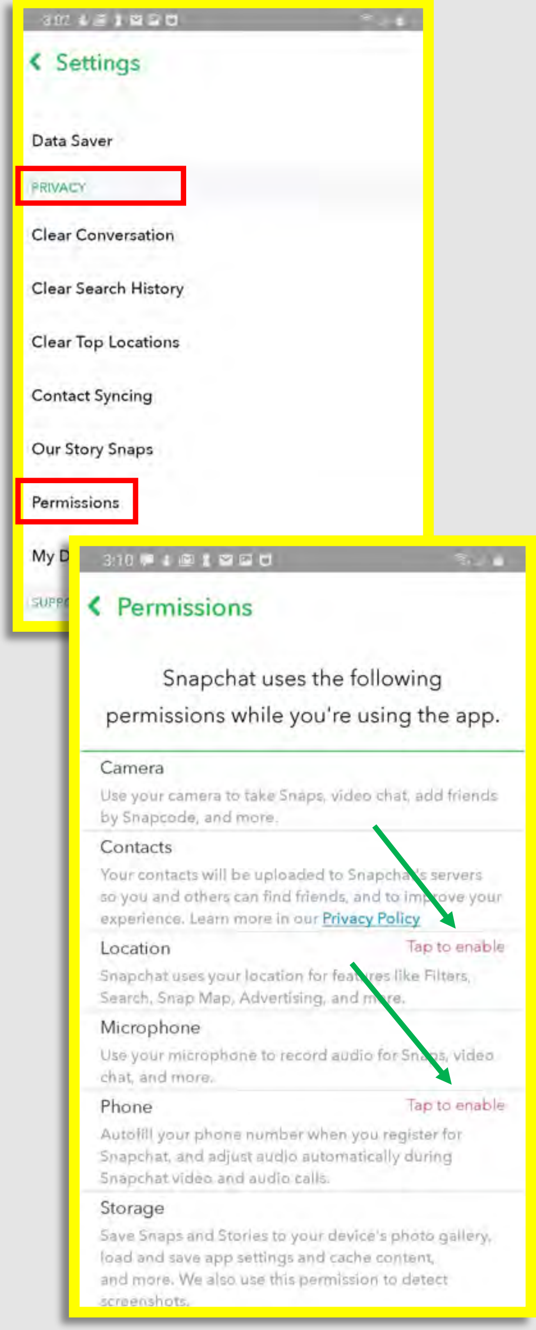
Permissions !

Ad Preferences

Lifestyle & Interests

Maps

Contacts



Settings

Data Saver

PRIVACY

Clear Conversation

Clear Search History

Clear Top Locations

Contact Syncing

Our Story Snaps

Permissions

My D

SUPP

Permissions

Snapchat uses the following permissions while you're using the app.

Camera
Use your camera to take Snaps, video chat, add friends by Snapcode, and more.

Contacts
Your contacts will be uploaded to Snapchat's servers so you and others can find friends, and to improve your experience. Learn more in our Privacy Policy

Location — Tap to enable
Snapchat uses your location for features like Filters, Search, Snap Map, Advertising, and more.

Microphone
Use your microphone to record audio for Snaps, video chat, and more.

Phone — Tap to enable
Autofill your phone number when you register for Snapchat, and adjust audio automatically during Snapchat video and audio calls.

Storage
Save Snaps and Stories to your device's photo gallery, load and save app settings and cache content, and more. We also use this permission to detect screenshots.

On Android (left): under "Settings", scroll down to the section titled "Privacy", then select "Permissions". You can adjust "Location" and "Phone". We recommend you leave them "Disabled", as seen here to the left.

What is "Scanning"? "Scan" lets you identify things like products, songs, barcodes, and more. To power this feature, Snap partners with third-parties like Amazon and Shazam. This means that if / when you "Scan", certain information may be sent to these partners. For example, Snap may send images captured by your camera to Amazon, who will send back search results if they find a matching product. Snap may send audio hashes captured by your microphone to Shazam, who will send back matching songs. The data is maintained for a minimal period of time and is not connected to your Snapchat account. Still, we do ***not*** recommend using the "Scan" feature.

UPDATED JAN 2021

LOCKING DOWN YOUR SNAPCHAT

According to TeenSafe.com 47 percent of users admit to using screenshots and 52 percent note that others have used screenshots of their messages. #Staysafeonline

Mobile Device Version

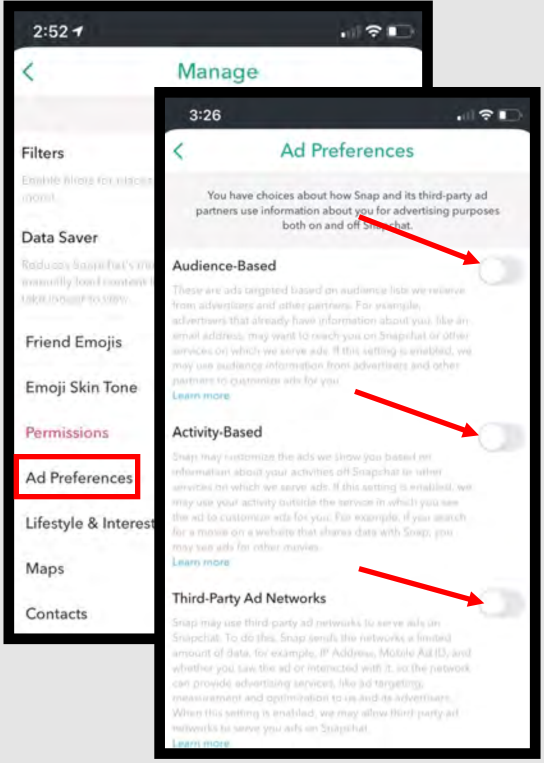
*** This information describes how to make your account secure on Android and iPhone mobile devices. Differences between iPhone Operating System (iOS) and Android Operating System (AOS) are significant for some features, and in these cases iPhone images are outlined **black** and Android **yellow**.*

Manage Advertising

Next, let's lock down what kinds of information Snapchat can capture from you in order to support advertising.

On iPhone: go back to the "Manage" section, select "Ad Preferences", ensure all three toggles are set to "Off"

On Android: under "Settings", scroll down to the section titled "Features", then select "Ads". Select "Ad Preferences" on the next screen, then ensure "Audience-Based", "Activity-Based", and "Third-Party Ad Networks" are all "Unchecked".



2:52

Manage

Filters

Enable filters for [illegible] more!

Data Saver

Reduces Snapchat's [illegible] manually load content [illegible] take longer to view.

Friend Emojis

Emoji Skin Tone

Permissions

Ad Preferences

Lifestyle & Interest

Maps

Contacts

3:26

Ad Preferences

You have choices about how Snap and its third-party ad partners use information about you for advertising purposes both on and off Snapchat.

Audience-Based

These are ads targeted based on audience lists we receive from advertisers and other partners. For example, advertisers that already have information about you, like an email address, may want to reach you on Snapchat or other services on which we serve ads. If this setting is enabled, we may use audience information from advertisers and other partners to customize ads for you.

Learn more

Activity-Based

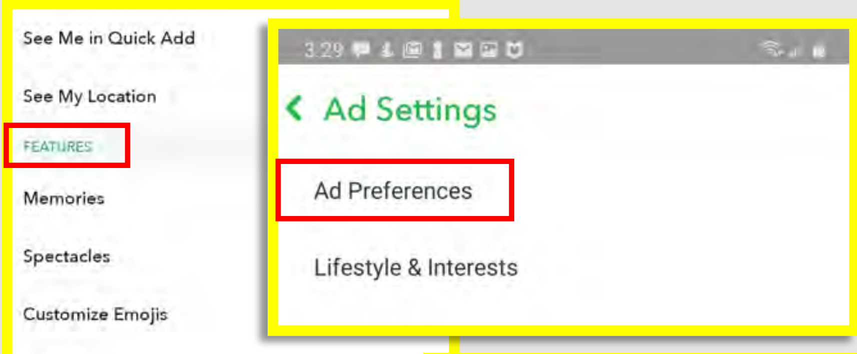
Snap may customize the ads we show you based on information about your activities off Snapchat or other services on which we serve ads. If this setting is enabled, we may use your activity outside the service in which you see the ad to customize ads for you. For example, if you search for a movie on a website that shares data with Snap, you may see ads for other movies.

Learn more

Third-Party Ad Networks

Snap may use third-party ad networks to serve ads on Snapchat. To do this, Snap sends the networks a limited amount of data, for example, IP Address, Mobile Ad ID, and whether you saw the ad or interacted with it, so the network can provide advertising services, like ad targeting, measurement and optimization to us and its advertisers. When this setting is enabled, we may allow third party ad networks to serve you ads on Snapchat.

Learn more



See Me in Quick Add

See My Location

FEATURES

Memories

Spectacles

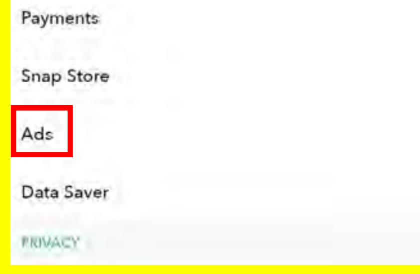
Customize Emojis

3:29

Ad Settings

Ad Preferences

Lifestyle & Interests



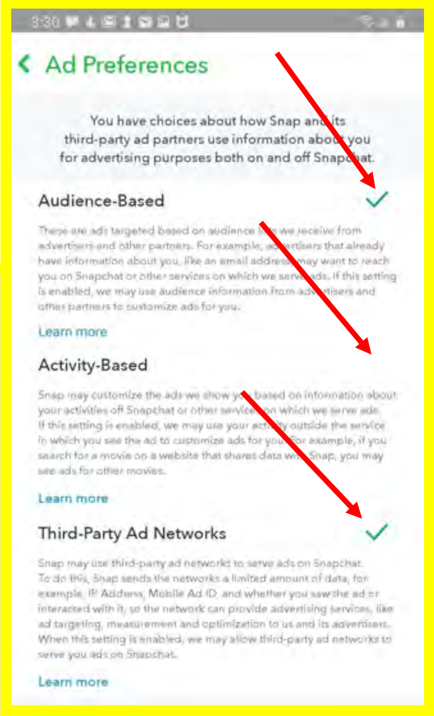
Payments

Snap Store

Ads

Data Saver

PRIVACY



3:30

Ad Preferences

You have choices about how Snap and its third-party ad partners use information about you for advertising purposes both on and off Snapchat.

Audience-Based ✓

These are ads targeted based on audience lists we receive from advertisers and other partners. For example, advertisers that already have information about you, like an email address, may want to reach you on Snapchat or other services on which we serve ads. If this setting is enabled, we may use audience information from advertisers and other partners to customize ads for you.

Learn more

Activity-Based

Snap may customize the ads we show you based on information about your activities off Snapchat or other services on which we serve ads. If this setting is enabled, we may use your activity outside the service in which you see the ad to customize ads for you. For example, if you search for a movie on a website that shares data with Snap, you may see ads for other movies.

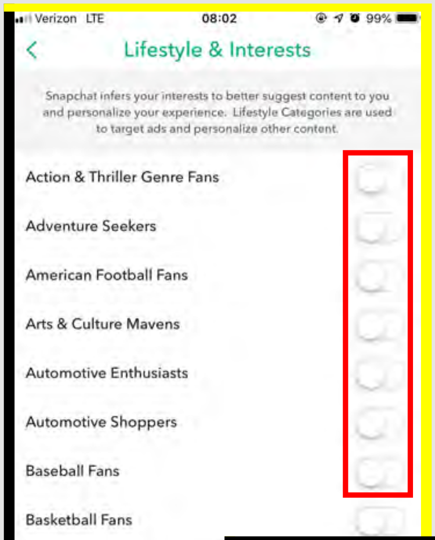
Learn more

Third-Party Ad Networks ✓

Snap may use third-party ad networks to serve ads on Snapchat. To do this, Snap sends the networks a limited amount of data, for example, IP Address, Mobile Ad ID, and whether you saw the ad or interacted with it, so the network can provide advertising services, like ad targeting, measurement and optimization to us and its advertisers. When this setting is enabled, we may allow third-party ad networks to serve you ads on Snapchat.

Learn more

Next, go back to the "Manage" section ("Ad Settings" on Android) and select "Lifestyle & Interests," its recommended that you unselect any section that is enabled. You can also periodically clear any tags that may have specified your interests by selecting "Clear Content Interests Tag" located at the very bottom of the "Lifestyle & Interests" screen.

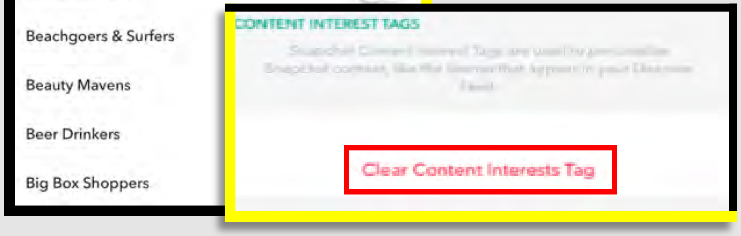


Verizon LTE 08:02 99%

Lifestyle & Interests

Snapchat infers your interests to better suggest content to you and personalize your experience. Lifestyle Categories are used to target ads and personalize other content.

- Action & Thriller Genre Fans
- Adventure Seekers
- American Football Fans
- Arts & Culture Mavens
- Automotive Enthusiasts
- Automotive Shoppers
- Baseball Fans
- Basketball Fans
- Beachgoers & Surfers
- Beauty Mavens
- Beer Drinkers
- Big Box Shoppers



CONTENT INTEREST TAGS

[illegible]

Clear Content Interests Tag

If you ever want to leave Snapchat for good, you can close your account on accounts.snapchat.com.

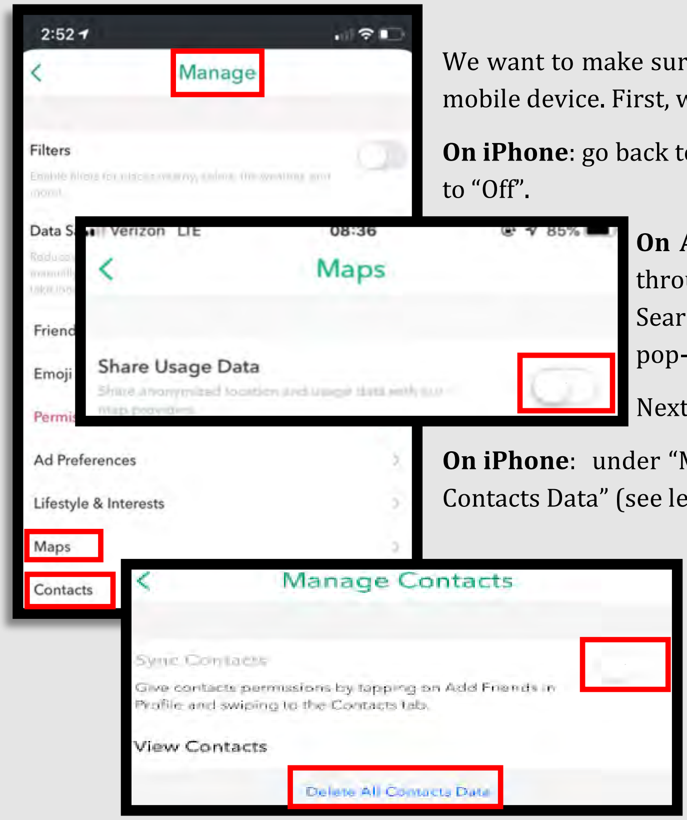
UPDATED JAN 2021

LOCKING DOWN YOUR SNAPCHAT

Mobile Device Version

*** This information describes how to make your account secure on Android and iPhone mobile devices. Differences between iPhone Operating System (iOS) and Android Operating System (AOS) are significant for some features, and in these cases iPhone images are outlined* ***black*** *and Android* ***yellow****.*

Manage Maps and Contacts



2:52

Manage

Filters

Data S

Friend

Emoji

Permis

Ad Preferences

Lifestyle & Interests

Maps

Contacts

Verizon LTE 08:36 85%

Maps

Share Usage Data

Share anonymized location and usage data with our map providers

Manage Contacts

Sync Contacts

Give contacts permissions by tapping on Add Friends in Profile and swiping to the Contacts tab.

View Contacts

Delete All Contacts Data

We want to make sure Snapchat cannot view your "Location" or the "Contacts" on your mobile device. First, we recommend you hide your location whenever possible.

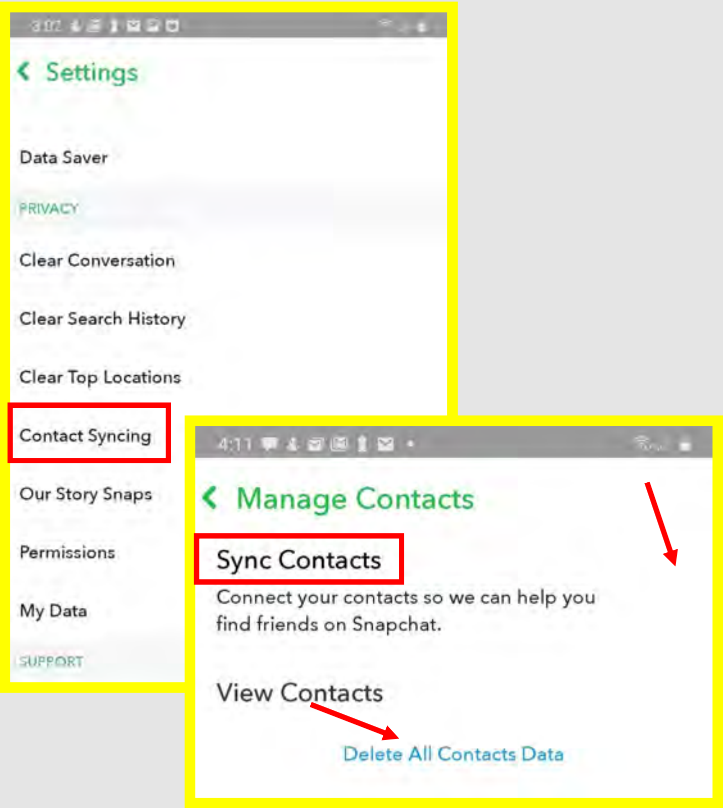
On iPhone: go back to "Manage", then "Maps". Set the toggle next to "Share Usage Data" to "Off".

On Android: go to "Settings", then scroll down to "Privacy", and go through all options listed, including "Clear Conversation", "Clear Search History", and "Clear Top Locations", and select "Clear" on the pop-up. This will clear location and other tracking data for you.

Next, we recommend forbidding Snapchat access to your "Contacts".

On iPhone: under "Manage", select "Contacts", then set toggle to "Off", and "Delete All Contacts Data" (see left).

On Android: under "Settings", scroll down again to "Privacy", select "Contact Synching". Ensure this feature is "Disabled" by identifying the space to the right of "Sync Contacts", and see that there is "No Checkmark" visible. Also, select "Delete All Contact Data" below "View Contacts" as well.



Settings

Data Saver

PRIVACY

Clear Conversation

Clear Search History

Clear Top Locations

Contact Syncing

Our Story Snaps

Permissions

My Data

SUPPORT

Manage Contacts

Sync Contacts

Connect your contacts so we can help you find friends on Snapchat.

View Contacts

Delete All Contacts Data

When does Snapchat delete "Snaps"? Snapchat servers are designed to automatically delete all "Snaps" (on their servers) after they have been viewed by all recipients. All unopened "Snaps" are deleted after 30 days.

61% of Snapchat users are female and 38% of users are male. This is opposite of Facebook and TikTok, which have majority male users. #Staysafeonline

UPDATED JAN 2021

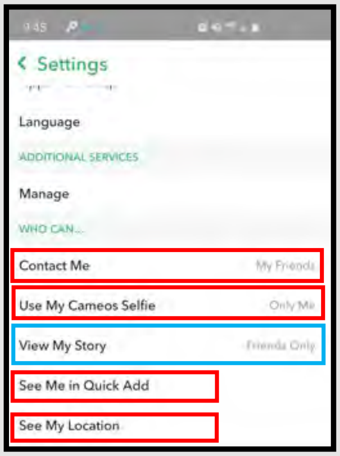
LOCKING DOWN YOUR SNAPCHAT

Mobile Device Version

*** This information describes how to make your account secure on Android and iPhone mobile devices. Differences between iPhone Operating System (iOS) and Android Operating System (AOS) are significant for some features, and in these cases iPhone images are outlined* ***black*** *and Android* ***yellow****.*

Manage Privacy Settings

Next it is important to set your privacy settings in order to control who can see your "Snaps" and contact you.



9:45

‹ Settings

Language

ADDITIONAL SERVICES

Manage

WHO CAN...

Contact Me — My Friends

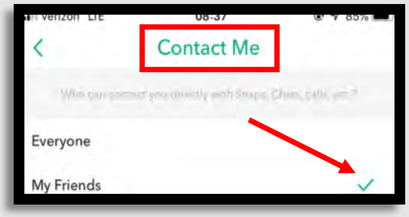
Use My Cameos Selfie — Only Me

View My Story — Friends Only

See Me in Quick Add

See My Location

On iPhone: go back to "Settings" and select "Contact Me" under the "Who Can…" section. It is recommended here that only "My Friends" are able to contact you, in order to help keep you and your children safer while using this App. Under the same "Who Can…" section select "View My Story" where it is also recommended that "My Friends" be enabled to ensure that your videos and pictures are not available to the public. Depending on your level of involvement (or your child's) with this App, you may also want to lock down the "See Me in Quick Add" section (shown to the right). Making sure this is ***not*** enabled will prevent your profile from showing up in other peoples' profiles as a suggested contact.



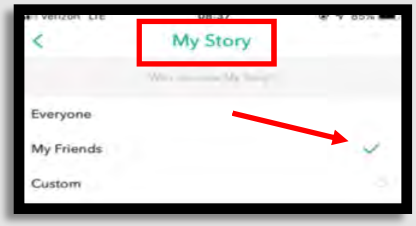
Verizon LTE 08:37 85%

‹ Contact Me

Who can contact you directly with Snaps, Chats, calls, etc.?

Everyone

My Friends ✓



Verizon LTE 08:37 85%

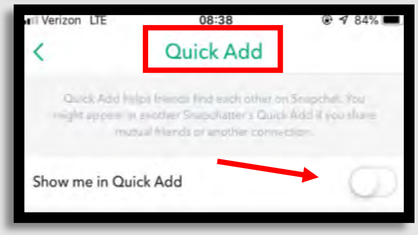
‹ My Story

Who can view My Story?

Everyone

My Friends ✓

Custom



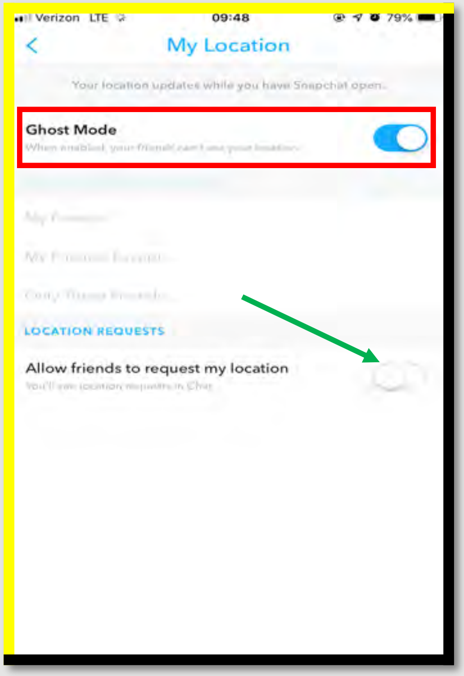
Verizon LTE 08:38 84%

‹ Quick Add

Quick Add helps friends find each other on Snapchat. You might appear in another Snapchatter's Quick Add if you share mutual friends or another connection.

Show me in Quick Add ○

On Android: go back to "Settings", scroll down to "Additional Services", and see "Contact Me", "View My Story", and "See Me in Quick Add", and set them to the same as noted above. (see right)



Verizon LTE 09:48 79%

‹ My Location

Your location updates while you have Snapchat open.

Ghost Mode ●
When enabled, your friends can't see your location.

My Friends

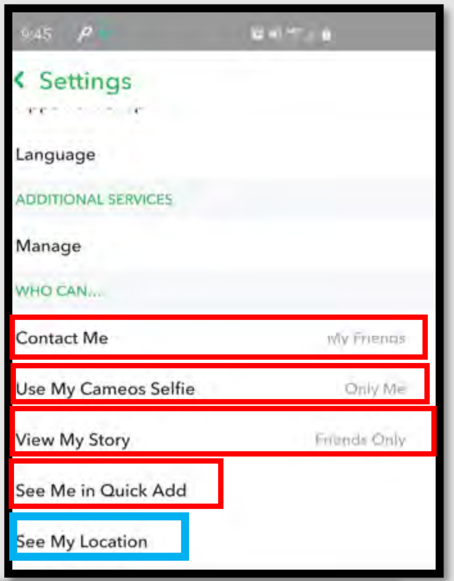
My Friends, Except...

Only These Friends...

LOCATION REQUESTS

Allow friends to request my location ○
You'll see location requests in Chat

Heading back to the "Settings" section, lets review the "See My Location", under the "Who Can " section on iPhone, and the "Additional Services" section on Android (see ***blue*** boxes above left and to the right). Snapchat allows users to use "Ghost Mode" to prevent even their "Friends" from viewing their location. We recommend you enable "Ghost Mode" in order to prevent anyone from viewing your precise location on the Snapchat "Map". We also recommend that you ***not*** enable "Allow friends to request my location."



9:45

‹ Settings

Language

ADDITIONAL SERVICES

Manage

WHO CAN...

Contact Me — My Friends

Use My Cameos Selfie — Only Me

View My Story — Friends Only

See Me in Quick Add

See My Location

What is "Snap Map"? "Snap Map" lets you see where your "Friends" are and what is going on around them. To open "Snap Map", pinch your fingers on the "Camera" screen, "Friends" screen, or "Discover" screen.

You won't appear on "Snap Map" until you open it for the first time and choose to share your location.

The FBI warns parents that pedophiles are using Snapchat to solicit images from young teens. These images are used for personal use or are sold to others.

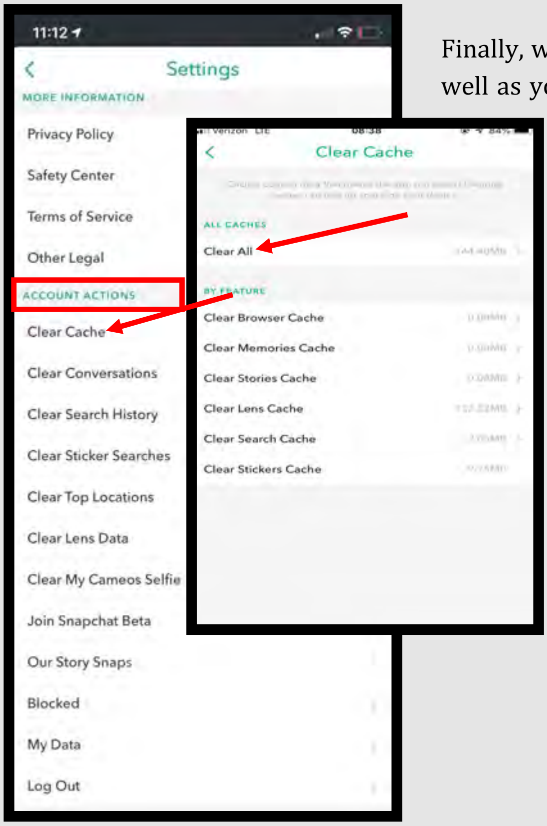
UPDATED JAN 2021

LOCKING DOWN YOUR SNAPCHAT

Mobile Device Version

*** This information describes how to make your account secure on Android and iPhone mobile devices. Differences between iPhone Operating System (iOS) and Android Operating System (AOS) are significant for some features, and in these cases iPhone images are outlined **black** and Android **yellow**.*

Because Snaps and messages disappear, it is impossible to monitor your child's behavior on Snapchat. Are they sexting peers? Are they bullying or being bullied?



11:12

Settings

MORE INFORMATION

Privacy Policy

Safety Center

Terms of Service

Other Legal

ACCOUNT ACTIONS

Clear Cache

Clear Conversations

Clear Search History

Clear Sticker Searches

Clear Top Locations

Clear Lens Data

Clear My Cameos Selfie

Join Snapchat Beta

Our Story Snaps

Blocked

My Data

Log Out

Clear Cache

ALL CACHES

Clear All

BY FEATURE

Clear Browser Cache

Clear Memories Cache

Clear Stories Cache

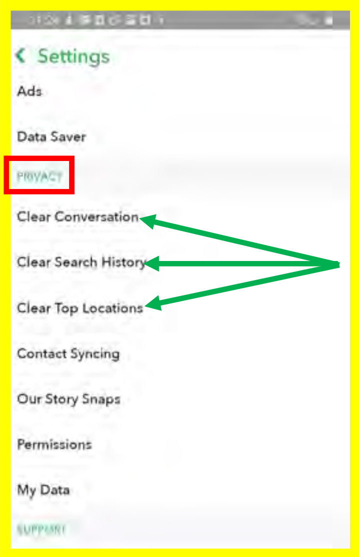
Clear Lens Cache

Clear Search Cache

Clear Stickers Cache

Finally, we recommend clearing out old data periodically on your Snapchat account, as well as your other social media accounts, whenever this feature is available. Snapchat provides you the capability to "Clear Cache", "Clear Conversations", Clear Search History, and "Clear Top Locations" (in addition to others on iPhone). You will clear these and the other options listed, the same way you would clear your Internet browser cache.

On iPhone: go back to "Settings", scroll down to "Account Actions", and choose which caches you want to clear. Alternatively we recommend "Clear Cache", then "Clear All", which will clear all caches under "Account Actions".



Settings

Ads

Data Saver

PRIVACY

Clear Conversation

Clear Search History

Clear Top Locations

Contact Syncing

Our Story Snaps

Permissions

My Data

SUPPORT

On Android: go back to "Settings" then "Privacy". Select each, "Clear Conversation", "Clear Search History", and "Clear Top Locations", and choose to "Clear" them. Each of these must be one separately and the options are fewer than offered on the iPhone.

Clear Chats: You can now unsend a sent message regardless of whether a recipient has seen it. This feature is different from "Clear Conversation", which only deletes content from your end. "Clear Chats" works in group chats or in one-on-one conversations, and applies to text, stickers, audio, or pictures and videos sent from your "Memories" section — not content you just took though. Note that the person in the conversation is alerted that a message was deleted. The purposes of the function are to clean up a typo and prevent unintentional messaging.

In order to delete a chat you already sent: 1) hold down the chat, and then 2) select "Delete". Once selected, Snapchat will provide another message box to confirm that you would like to delete the chat you have just selected, and to remind you that, although the message is being deleted, your friends will still be able to see that something was deleted, if not the deleted content itself.

UPDATED JAN 2021

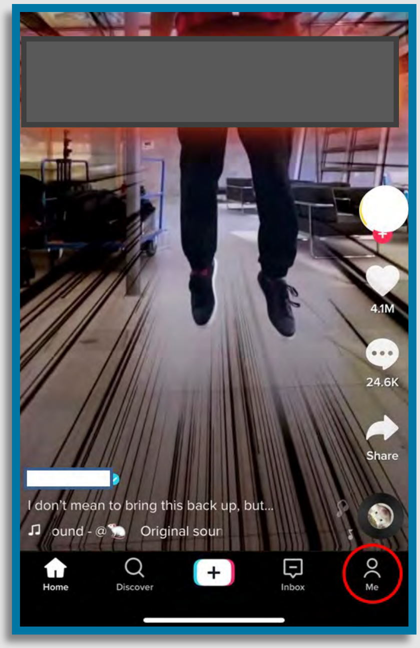
TikTok SMART CARD

Do's and Don'ts

- ***Do*** opt out of personalized data. TikTok is owned by a company based in China, opting out helps prevent your data from being gathered and redistributed without your knowledge.
- ***Do*** ensure family members take similar precautions with their accounts. Their privacy and share settings can expose your personal data.
- ***Do*** use a picture of something other than yourself for your profile photo. Profile photos are viewable to the public.
- Do ***not*** provide any identifiable information (e.g. name, hobbies, job title, etc.) on your profile or in your videos.
- Do ***not*** link your TikTok account to any third party applications such as Facebook, LinkedIn, Instagram or Twitter.
- Do ***not*** use default settings on TikTok. All default settings are set to allow "Everyone" to be able to view and comment on your videos.
- Do ***not*** use identifiable locations, backgrounds or relatable images, when posting videos. It is important to be aware of your surroundings when posting images.

TikTok can loosely be described as a social network for amateur videos, teenagers and young people are the primary users of the app. It is easy for random people to reach out to users, especially teens, for nefarious reason. Recently TikTok has attempted to fix this issue by updating it's privacy settings, as noted throughout this card. Understand that TikTok is owned by a Chinese-based company, and it is thus important to limit what personal information you include on your account, videos and posts.

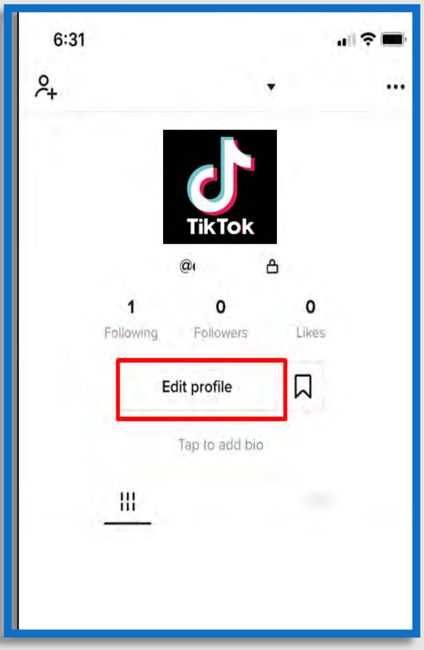
** This information describes how to make your TikTok account secure on Android and iPhone mobile devices. Most images provided are of Android screens. Differences between iPhone Operating System (iOS) and Android Operating System (AOS) are minimal - when they are significant, such differences are noted specifically.



Edit Profile

When opening a new application, the first thing you want to do is set up your privacy settings in order to protect your personally identifiable information (PII). Default settings in Tik Tok are set to allow everyone to view, comment and access the information you post.

To begin locking down your account, look to the lower right hand corner and select "Me" to go to your profile settings (highlighted to the left in red). Click on the "Edit Profile" button. We recommend you do not use personal images or photos of yourself or your family. We also recommend you leave your "Bio" information blank or put as little personal information there as possible.



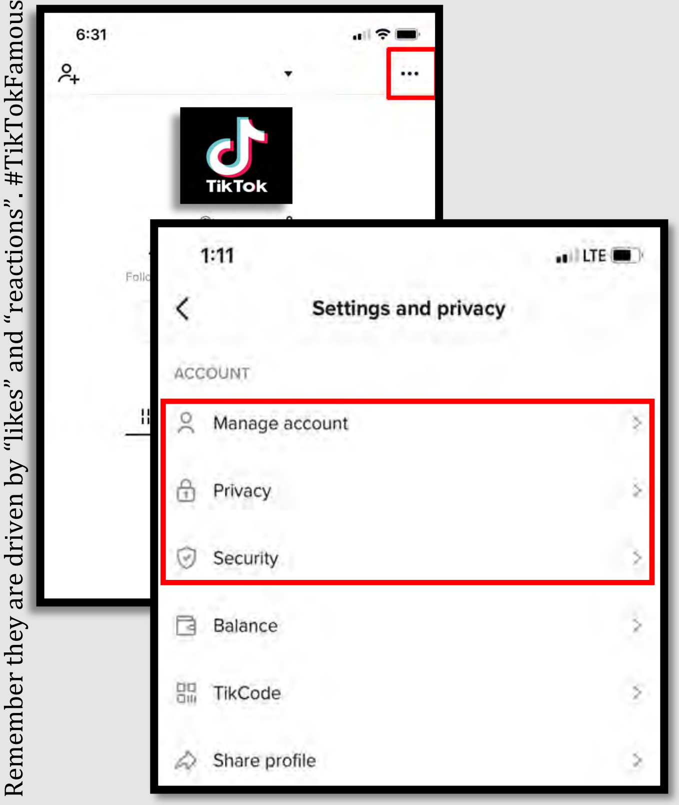
Shut Off Direct Messaging so that strangers cannot attempt to message you (or your children). Select the "Settings" icon, select "Privacy and safety", select "Who can send me messages", select either "Friends" or "Off".

We recommend you do ***not*** link your account to any other social media platform (e.g. Twitter, Instagram, Facebook), as TikTok will pull in your personally identifiable information and pictures from the other platforms. We also recommend you avoid using any Personally Identifiable Information (PII) anywhere on your profile. You are not required to put any personal or biographical information into your profile, and it is recommended you leave this section blank. PII is often used as a means to gain access to certain accounts (e.g. banks, credit cards, schools). Providing even just your birthday could help an identity thief steal your identity.

TikTok is a video-sharing social networking service owned by ByteDance, a Beijing-based company.

UPDATED JAN 2021

TikTok SMART CARD

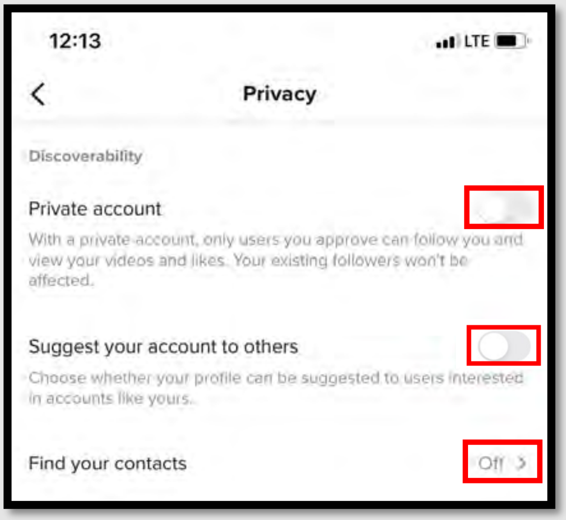


Account Privacy & Login Information

To the left you will notice the "Settings and privacy" menu. There are several items to be reviewed from this menu, of importance are the "Privacy" section as well as the "Security" section. Other parts of this menu will be discussed later on in this card.

First, you will need to lock down your login information and set your account privacy. In order to access the "Settings and Privacy" tab go back to your "Profile" page and select the "Menu" button, (three horizontal lines on iPhone, 3 vertical lines on Android) in the upper right hand corner of your "Profile" screen (highlighted to the left). Under "Account", select "Manage my account". We recommend you set the "Save login info" toggle to "Off" in order to ensure that, should you lose your mobile device, no one has access to your TikTok account.

By default, all accounts are set to "Public", which means anyone can see what you post on Tik Tok. We recommend you set your account to "Private account", which will ensure that all videos can only be seen by the creator and no one else on the platform. With a "Private account" you can approve or deny users and limit incoming messages to "Friends" only. Note that even with a "Private account", your "Photo", Username" and "Bio" are still visible to all users of the platform. We recommend you set "Suggest your account to others" to "Off", which will allow you more agency in choosing and accepting your followers more proactively.



Private account

With a private account, only users you approve can follow you and view your videos and likes. Your existing followers won't be affected.

Suggest your account to others

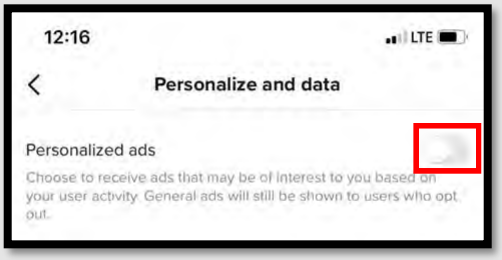
Choose whether your profile can be suggested to users interested in accounts like yours.

Find your contacts Off

In order to make your account "Private" go to "Privacy", under "Settings and Privacy", then set "Private account" toggle to "On", and "Suggest your account to others" toggle to "Off" (see left). As always it is recommended that you do not allow Tik Tok or any other social media account to have access to your contacts, if this section is marked "on" simply select it and toggle to "off."

Next, review the "Personalization and Data" section. Here you will want to make sure you toggle "Ad Authorization" to off and then select "Personalization and data." We recommend not allowing Personalized ads from Tik Tok, simply toggle to turn off this function.

Parents: Keep in mind that children may be tempted to take risks to get more of a following or get "likes" on a video, so it's important to talk with them about what they share and with whom. Also, users can "like" or "react" to a video, follow an account, or send messages to each other. This means that there is a risk that strangers will be able to directly contact children on the app.



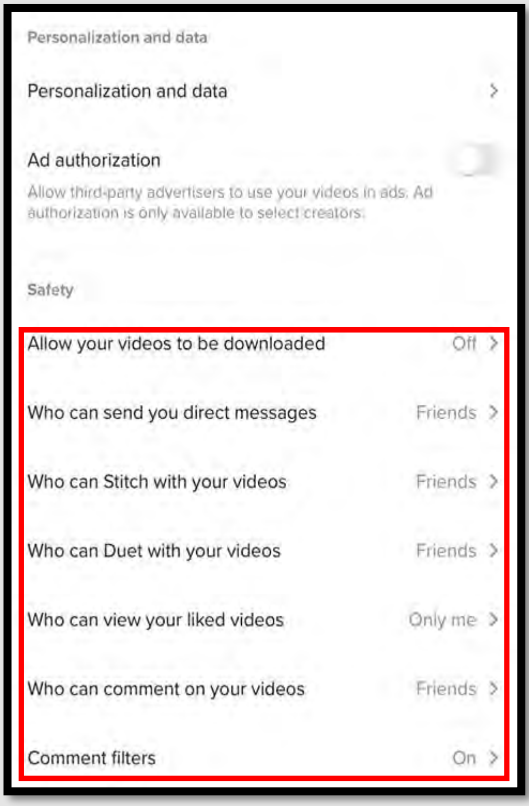
Personalized ads

Choose to receive ads that may be of interest to you based on your user activity. General ads will still be shown to users who opt out.

Talk with your children about what kinds of videos are okay to share, and with whom. Remember they are driven by "likes" and "reactions". #TikTokFamous

UPDATED JAN 2021

TikTok SMART CARD


Personalization and data

Personalization and data >

Ad authorization

Allow third-party advertisers to use your videos in ads. Ad authorization is only available to select creators.

Safety

Allow your videos to be downloaded — Off >

Who can send you direct messages — Friends >

Who can Stitch with your videos — Friends >

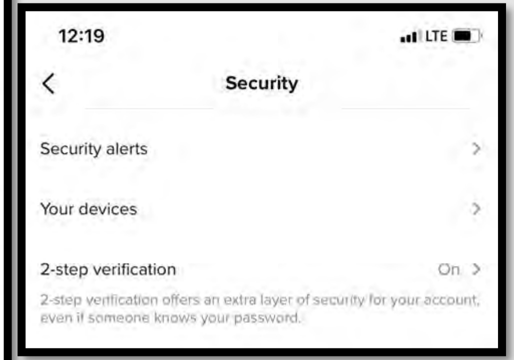
Who can Duet with your videos — Friends >

Who can view your liked videos — Only me >

Who can comment on your videos — Friends >

Comment filters — On >

Continuing on, look to the "Safety" section within the "Privacy" menu. Next it is recommended that you turn off the "Ad authorization" in Tik Tok. Here you will want to go through each section here so that you can maintain privacy on your Tik Tok. It is highly recommended that the highest level of openness on Tik Tok be "Friends" where no setting is "everyone." This is due in part to Tik Tok's ownership, discussed on the first page, but also in part due to the type of individual that could presumably contact you via Tik Tok. Predators have been known to reach out to people and blackmail them using Tik Tok's direct messaging service. Additionally, it is strongly recommended that you do not allow others to download your videos, these may end up on sites and in places you would rather they not. For all recommendations within the "Safety" section see the picture on the left.


12:19 LTE

Security

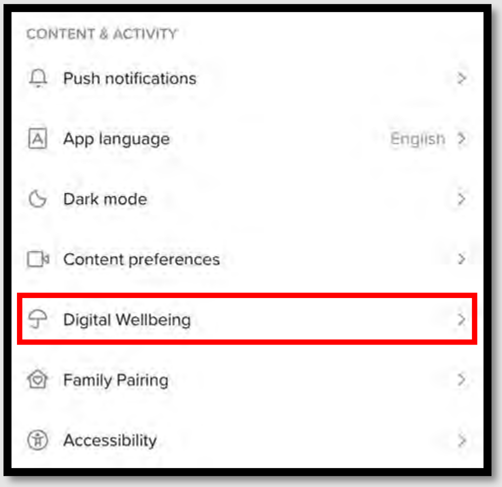
Security alerts >

Your devices >

2-step verification — On >

2-step verification offers an extra layer of security for your account, even if someone knows your password.

Now, head back to the "Settings and privacy" and select "Security." Here you can check if there have been any suspicious activity on your Tik Tok account and set up "2-step verification." Like all other accounts, setting up 2 step verification is extremely important. Additionally, it is important periodically to check in here and make sure your account is secure.


CONTENT & ACTIVITY

Push notifications >

App language — English >

Dark mode >

Content preferences >

Digital Wellbeing >

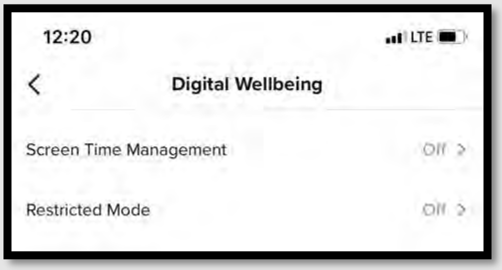
Family Pairing >

Accessibility >

Much like YouTube, Tik Tok has created a "Restricted Mode" for children or teenagers whose parents want to limit the type of content they can see and follow. Considering some of the content on Tik Tok it might be a good idea to utilize this function if you have young preteens or teenagers that have access to this app.

In order to turn the "Restricted Mode" for Tik Tok head back to your main menu, "Settings and privacy," and scroll towards the middle of the menu (shown to the left) and select "Digital Wellbeing." From there select "Restricted Mode" then select "Turn on Restricted Mode" from the bottom of your screen. In order to prevent this mode from being turned off by your teenager you can create a passcode to turn this mode off.

From the "Digital Wellbeing" menu you can also manage your child's screen time if you so choose.


12:20 LTE

Digital Wellbeing

Screen Time Management — Off >

Restricted Mode — Off >

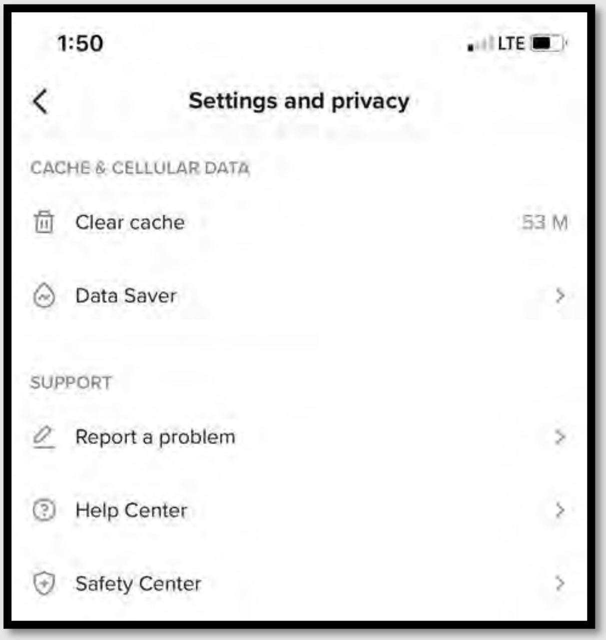
Duets can be a fun way to create videos with another user, but you must be in control - Tik Tok gives you the option to **decide who can make duets with you** (everyone, no one, or just friends). We recommend you choose "Friends".

If your account is locked down, you're doing GREAT! If you allow your videos to be downloaded, you run the risk of compromising personal information.

UPDATED JAN 2021

TikTok SMART CARD

Parents have expressed concern about the inappropriate language and content of some videos posted on Tik Tok, which may make it less suitable for younger children.



1:50 LTE

Settings and privacy

CACHE & CELLULAR DATA

Clear cache 53 M

Data Saver

SUPPORT

Report a problem

Help Center

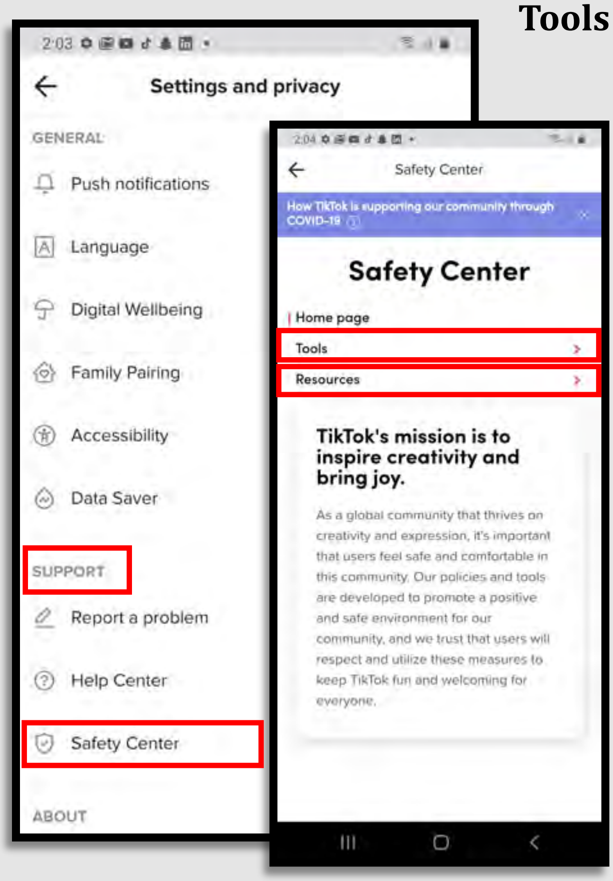
Safety Center

In order to save on space and clear any unwanted cache Tik Tok allows you to periodically delete caches and downloads. For IPhone users simply scroll to the bottom half of the main menu and select “Clear cache”. For Android users simply scroll to the lower portion of the main menu and select “Free up space” then select “Clear” from the right hand side of your screen.

Notice from the picture on the left hand side of this card that you can also select a “report a problem” icon. Here you are able to get help with things like logging in, reporting an account, and recovering lost or stolen passwords. Always remember if you feel your account has been hacked, you need to change your password to your Tik Tok account as well as the email account that is associated with your Tik Tok account to be on the safe side.

Safety Center:

Tools and Resources



2:03

Settings and privacy

GENERAL

Push notifications

Language

Digital Wellbeing

Family Pairing

Accessibility

Data Saver

SUPPORT

Report a problem

Help Center

Safety Center

ABOUT

2:04

Safety Center

How TikTok is supporting our community through COVID-19

Safety Center

Home page

Tools

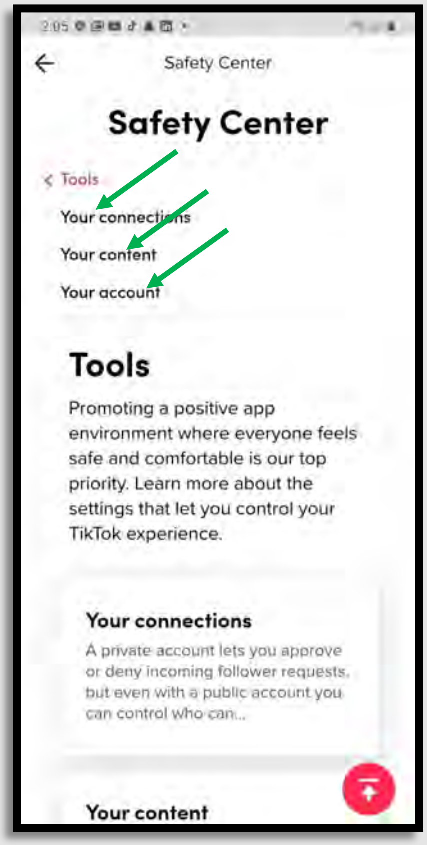
Resources

TikTok's mission is to inspire creativity and bring joy.

As a global community that thrives on creativity and expression, it's important that users feel safe and comfortable in this community. Our policies and tools are developed to promote a positive and safe environment for our community, and we trust that users will respect and utilize these measures to keep TikTok fun and welcoming for everyone.

Finally, let’s visit Tik Tok’s “Safety Center”, which is a useful resource hub that will help you learn how to use Tik Tok in the most safe and enjoyable way. In this section, you will find “Tools” and “Resources” that will help you further navigate your content, security, and privacy options. First, find the “Safety Center” by going to “Settings and privacy”, scroll to the middle of the menu and select “Safety Center” in the “Support” section.

Next, select “Tools”, and you will be given options to explore how to maximize your control over your “Connections”, your “Content”, and your “Account”.



2:05

Safety Center

Safety Center

< Tools

Your connections

Your content

Your account

Tools

Promoting a positive app environment where everyone feels safe and comfortable is our top priority. Learn more about the settings that let you control your TikTok experience.

Your connections

A private account lets you approve or deny incoming follower requests, but even with a public account you can control who can...

Your content

UPDATED JAN 2021

TikTok SMART CARD

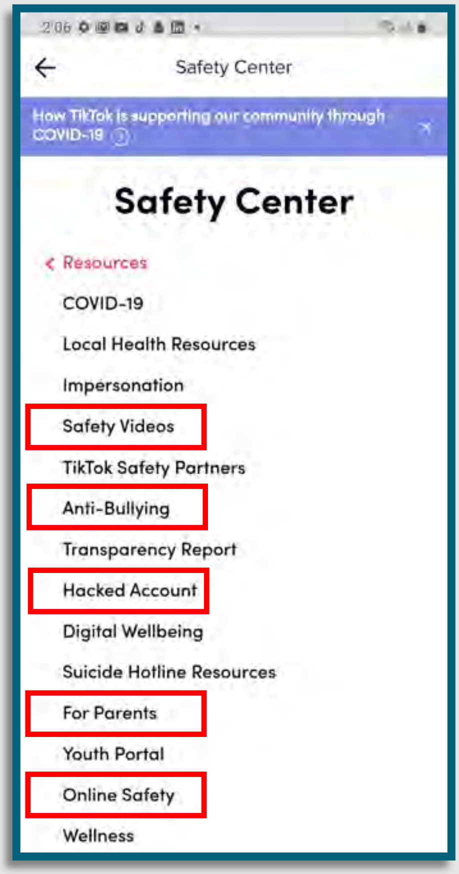
By changing all the safety settings for TikTok to "Friends" you are protecting your account from just anyone finding, commenting or contacting you or your child.

Safety Center: Tools and Resources, ctd.

Back under "Safety Center", select "Resources" and see a list of various resources you will find useful. We recommend you check out "Safety Videos" (see right), and the "You're in Control" video series, which are short educational Tik Tok videos on topics, many of which are presented in this SmartCard, such as "Choosing who can duet with you", Reporting inappropriate behavior", etc.

Also, check out the "Anti-Bullying" information, which explains what steps you can take to make sure you (or your child) are not receiving unwanted community interactions, as well as what you can do if you find yourself in a bullying situation.

Next, if you are a parent, do check out the "For Parents" link, which offers more explanation about what Tik Tok is meant to be and how to keep your child safe on Tik Tok. For instance, this section explains that Tik Tok is for children 13 years and older, but that in the U.S. children under 13 may register for a "Child Account", which restricts posting and interactions on the platform. "Family pairing" and "Account Privacy" options are further explained as tools to help keep teens safe on Tik Tok. We recommend you visit the link and employ all recommendations suggested to keep you and your family safe.



2:06

Safety Center

How TikTok is supporting our community through COVID-19

Safety Center

< Resources

COVID-19

Local Health Resources

Impersonation

Safety Videos

TikTok Safety Partners

Anti-Bullying

Transparency Report

Hacked Account

Digital Wellbeing

Suicide Hotline Resources

For Parents

Youth Portal

Online Safety

Wellness

Report a Problem

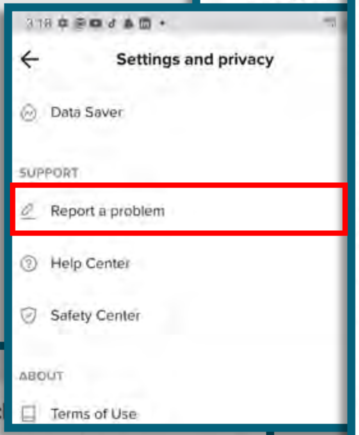
Tik Tok has "Community Guidelines" that outline the types of behavior it considers counter to its values. Content that violates these guidelines can be reported, removed, and reported to legal authorities. You can access the "Community Guidelines" via the "Safety Center" on Tik Tok. But if you see content you think should be reported, you can do the following: under "Settings and privacy", select "Report a problem", then scroll to the bottom of the "Feedback and help" page that appears, and select "Abuse Report". Select "How to report" and follow the rest of the prompts.

Community Guidelines

Last Updated, January, 2020

TikTok's mission is to inspire creativity and bring joy. We are building a global community where users can create and share authentically, di

and connect wi



3:18

Settings and privacy

Data Saver

SUPPORT

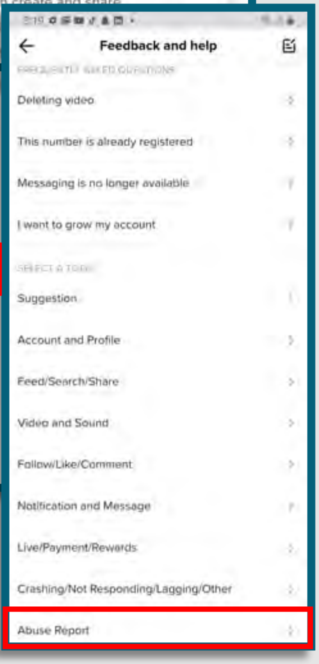
Report a problem

Help Center

Safety Center

ABOUT

Terms of Use



3:19

Feedback and help

FREQUENTLY ASKED QUESTIONS

Deleting video

This number is already registered

Messaging is no longer available

I want to grow my account

SELECT A TOPIC

Suggestion

Account and Profile

Feed/Search/Share

Video and Sound

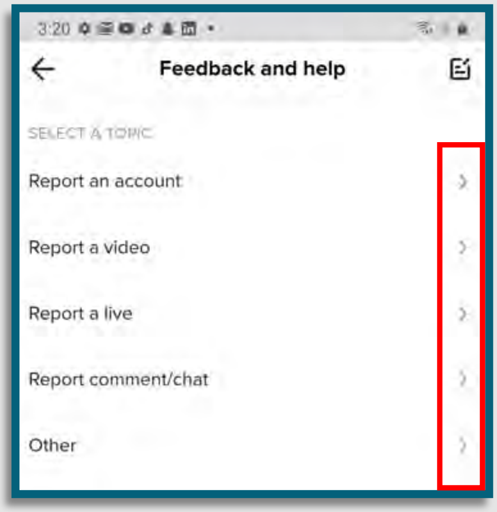
Follow/Like/Comment

Notification and Message

Live/Payment/Rewards

Crashing/Not Responding/Lagging/Other

Abuse Report



3:20

Feedback and help

SELECT A TOPIC

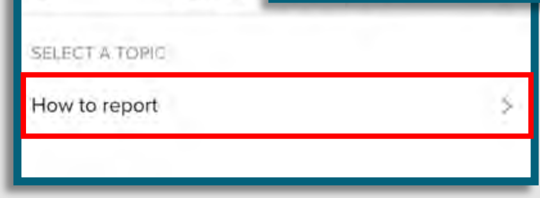
Report an account

Report a video

Report a live

Report comment/chat

Other



3:19

Feedbac

SELECT A TOPIC

How to report

UPDATED JAN 2021

TikTok SMART CARD

Indicators of Possible Account Compromise:

Your TikTok account may have been hacked, if you experience following suspicious behavior:

- Change of your password, security email and associated phone number.
- Change of your username or nickname.
- Deleting / Posting videos without your permission.
- Sending messages you did not write.

If you suspect your account has been compromised, please follow the steps below to keep your account secure:

Change Password: In TikTok, a hacker will be automatically kicked out of your account after changing the password.

Check account information to determine if it is accurate: Select "Manage My Account" option under the TikTok settings, check if the associated account information is accurate. If you cannot change password by yourself, please contact TikTok via their In-app Feedback (App settings – Report a Problem). You may follow the steps shown below to change the password and verify account information.

- Tap on "…" for 'Privacy & Settings'
- Go to 'Manage My Account'
- Select password to change and other account information to verify

If you need to report **Spam/Fake Accounts/Harassment**: Go to https://support.tiktok.com/en

If your account was hacked: https://www.tiktok.com/safety/resources/hacked-account?lang=en&appLaunch=web and reach out to TikTok and notify them of your hacked account at https://www.tiktok.com/about/contact?lang=en

Also, if you find any bullying or inappropriate behavior TikTok has information at site https://www.tiktok.com/safety/resources/anti-bully?lang=en&appLaunch=web

If you cannot log in to your email account, Twitter has provided links to each email accounts "having trouble signing in" page for your convenience. https://help.twitter.com/en/managing-your-account/cant-access-my-accounts-email-address

Important Message from TikTok: If you have a public profile, anyone signed into TikTok can view your public videos. However, only approved followers can send you a message. Whether you choose to have a public or a private account, you can always: block another from contacting you at any time; save a video privately so content will not be viewable by any other user; filter comments; "manage" your duets.

Tips to keep your account safe:

1. Never trust 3rd-party websites that promise to give away free likes, fans, crowns, coins, or other incentives as they may be able to take your login info.

2. Select a secure password that contains at least one number and one special character.

Make sure your options for "Who can download my video" are set to "Nobody". Otherwise other users can download and share your videos. #lockitdown

UPDATED JAN 2021

LOCKING DOWN YouTube

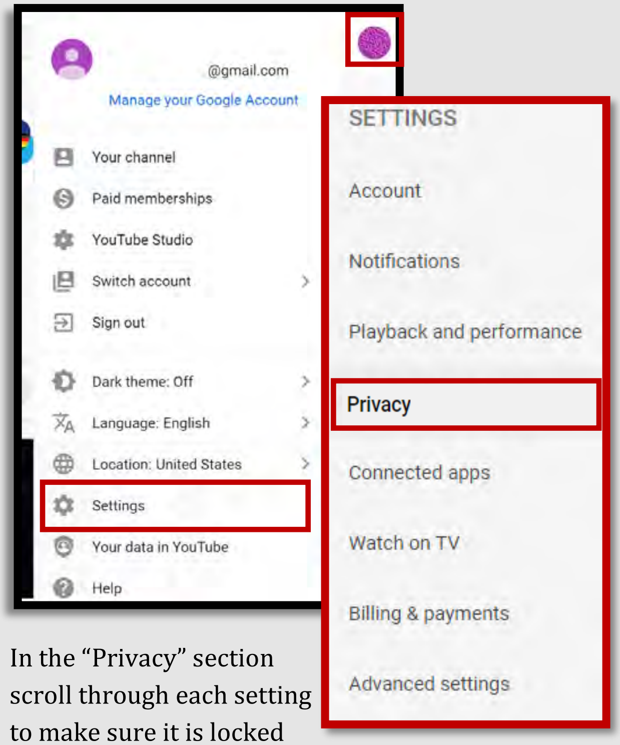
Personal Computer (PC) Version

Do's and Don'ts

- Do monitor the videos that your children are watching, even if they are in "Restricted Mode."
- Do use Two-Factor Authentication to protect all your information. Enable this function via your Google Account.
- Do set all your videos to "Unlisted" or "Private" so that you maintain full control over who can see them.
- Do ***not*** allow your children to post "Public" videos to their YouTube account. Posting public videos allows "subscribers" (strangers) to follow your children on YouTube.
- Do ***not*** ignore the "Comments" and feedback on your published videos. Review them to make sure they don't reveal any personal information about you.

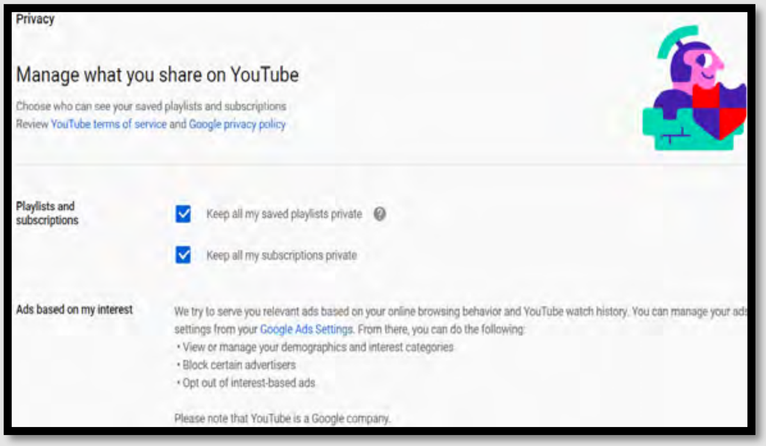
YouTube is a video sharing service with which users can create their own profile, upload videos, watch, react to, and comment on other videos. Created in 2005, YouTube is now one of the most popular sites on the Internet.

*** This SmartCard provides guidance on how to secure your YouTube account on personal computer (PC) and mobile devices, both iPhone and Android. PC instructions are followed by mobile device instructions below.*



Privacy Settings

Your "YouTube Account" (if you have one) is connected to your "Google Account", meaning your Google email and password are used to sign into YouTube. To set your security and privacy settings on YouTube, let's begin with "Settings". Look to the top right of your screen and select your "Google Profile" picture (see left). From the dropdown menu, select "Settings", and the "Settings" menu will appear. Select "Privacy".



Privacy

Manage what you share on YouTube

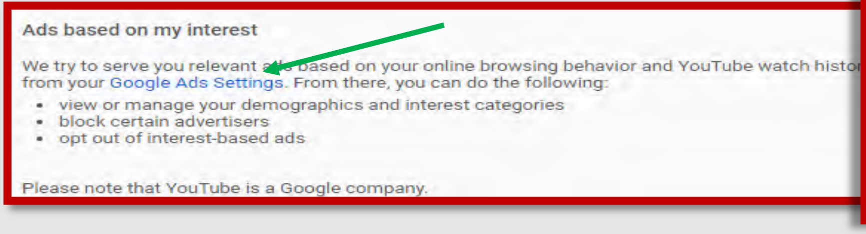
Choose who can see your saved playlists and subscriptions
Review YouTube terms of service and Google privacy policy

Playlists and subscriptions
☑ Keep all my saved playlists private
☑ Keep all my subscriptions private

Ads based on my interest
We try to serve you relevant ads based on your online browsing behavior and YouTube watch history. You can manage your ads settings from your Google Ads Settings. From there, you can do the following:
- View or manage your demographics and interest categories
- Block certain advertisers
- Opt out of interest-based ads

Please note that YouTube is a Google company.

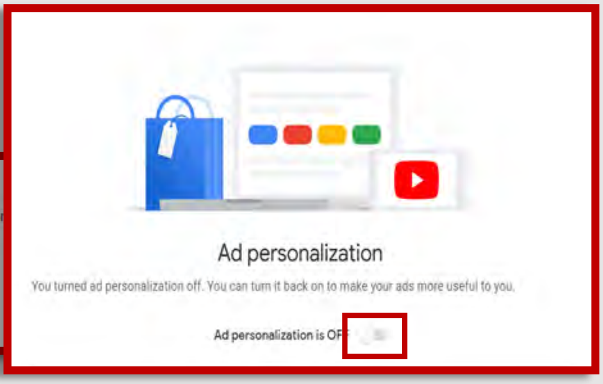
In the "Privacy" section scroll through each setting to make sure it is locked down. We recommend you keep all sections in "Manage what you share on YouTube" private, set the toggles to "On" or "Check" the boxes. In the section "Ads based on my interest", we recommend turning this feature off, as in order for it to function it must collect data from you. Disable the "Google Ads Settings" by selecting "Google Ads Settings", then set the toggle to "Off" as seen below.



Ads based on my interest

We try to serve you relevant ads based on your online browsing behavior and YouTube watch histor
from your Google Ads Settings. From there, you can do the following:
- view or manage your demographics and interest categories
- block certain advertisers
- opt out of interest-based ads

Please note that YouTube is a Google company.



Ad personalization

You turned ad personalization off. You can turn it back on to make your ads more useful to you.

Ad personalization is OFF

YouTube looks like it refreshes after that last step, but you'll still see the same content as you did before if you don't refresh your screen. #themoreyouknow

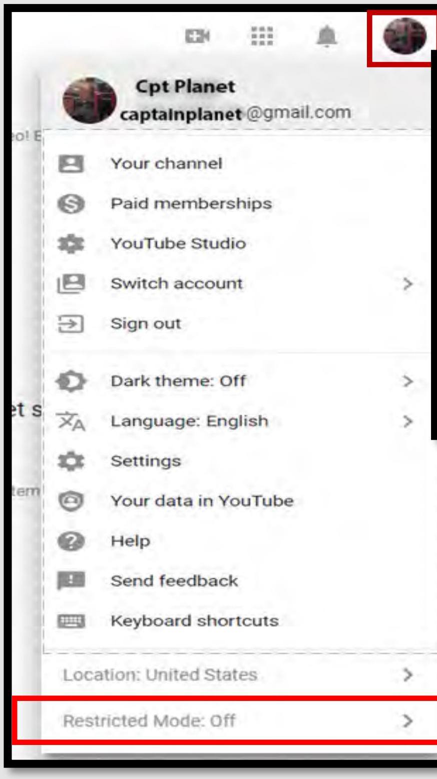
UPDATED JAN 2021

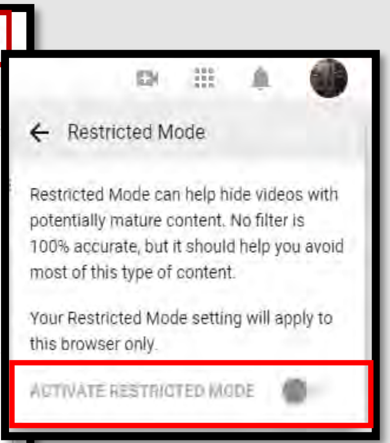
LOCKING DOWN YouTube

Personal Computer (PC) Version

Restrict Mature Content

Parents, are you concerned with what your children are watching on YouTube? “Restricted Mode” can help you ensure they are not being presented mature content. To enable this feature, select your “Google Profile” icon again. On the dropdown, you will need to scroll to the very bottom, select “Restricted Mode”, set the toggle to “On”.



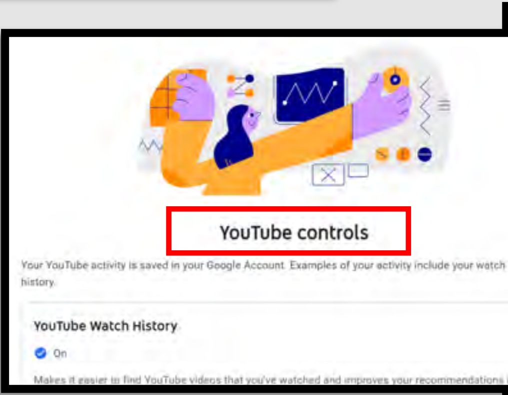


Restricted Mode can help hide videos with potentially mature content. No filter is 100% accurate, but it should help you avoid most of this type of content.

Your Restricted Mode setting will apply to this browser only.

Delete History

Another important feature located at the bottom of your “Account Menu” (from your “Google Profile” icon) is the “Your data in YouTube” tab. Just as it is important to clear your browser history on your search engines, it is important to manage and clear your history on your YouTube account. Select “Your data in YouTube”. On the next page, scroll down to “YouTube Controls”, select “Manage your YouTube Watch History”. (see below, green arrow)

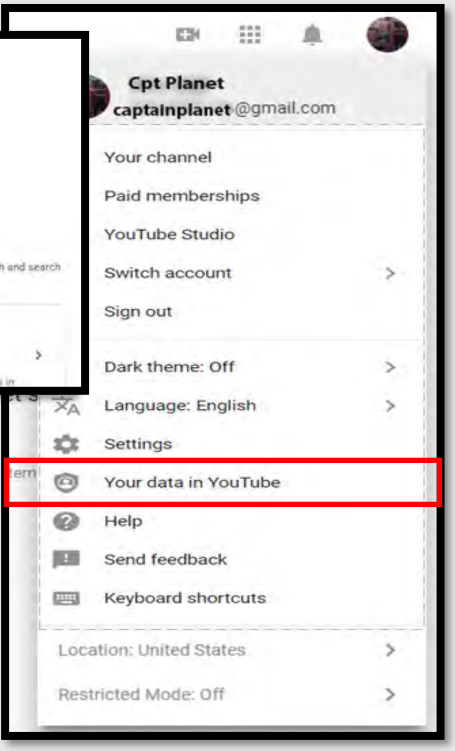


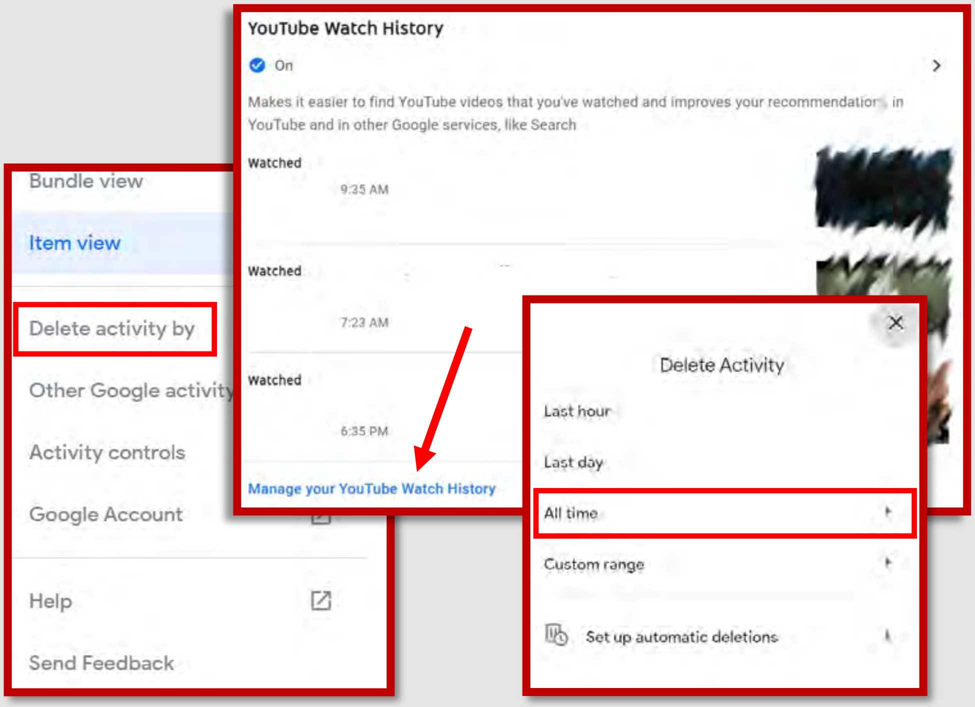
Your YouTube activity is saved in your Google Account. Examples of your activity include your watch and search history.

YouTube Watch History

On

Makes it easier to find YouTube videos that you've watched and improves your recommendations in





YouTube Watch History

On

Makes it easier to find YouTube videos that you've watched and improves your recommendations in YouTube and in other Google services, like Search

Watched 9:35 AM

Watched 7:23 AM

Watched 6:35 PM

From “Manage your YouTube Watch History” a new page will load (see left). Look to the left of your screen to see a menu of available options to manage and delete your history. We recommend you select “Delete activity by”, then select “All time”, which will delete your entire history. You can also set up automatic deletions and YouTube will delete your history according to the schedule you designate.

Set up automatic deletions to have YouTube delete your watch and search histories automatically, or delete manually. #themoreyouknow

UPDATED JAN 2021

LOCKING DOWN YouTube

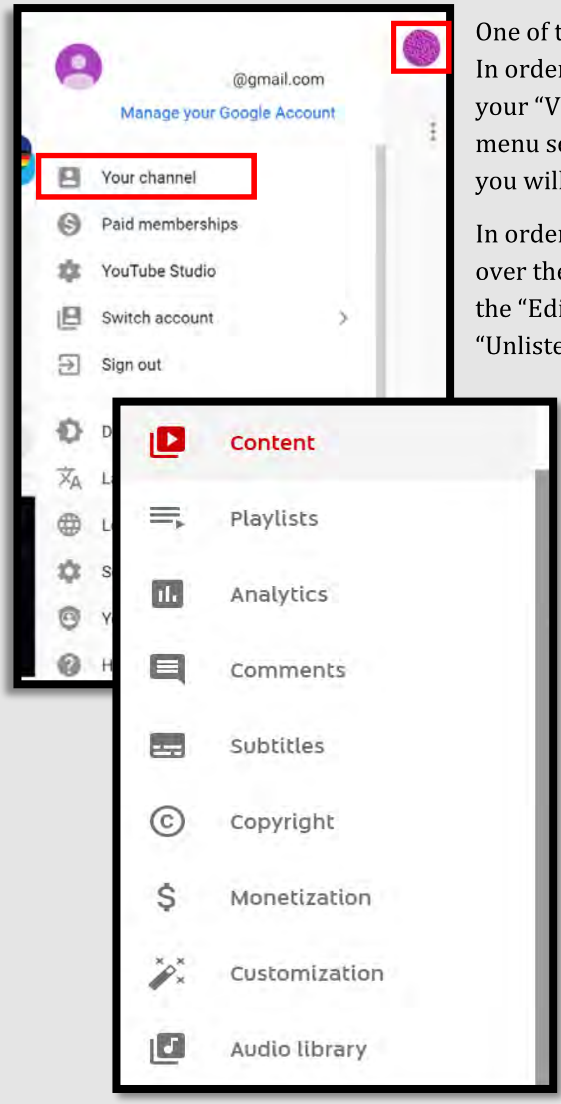
Personal Computer (PC) Version

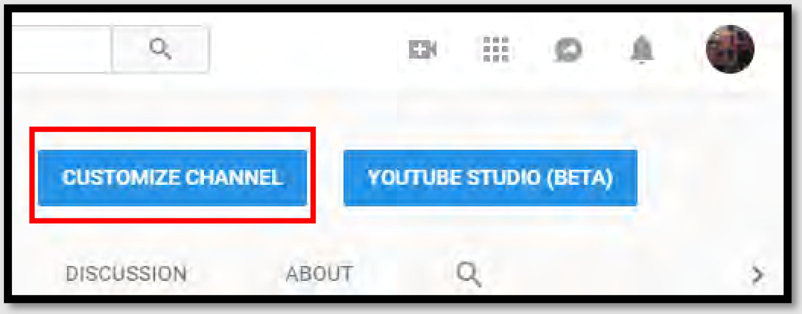
Restricted Mode doesn't catch everything, and it's easy to disable. It is important to check on your children and even teenagers while they are using YouTube.

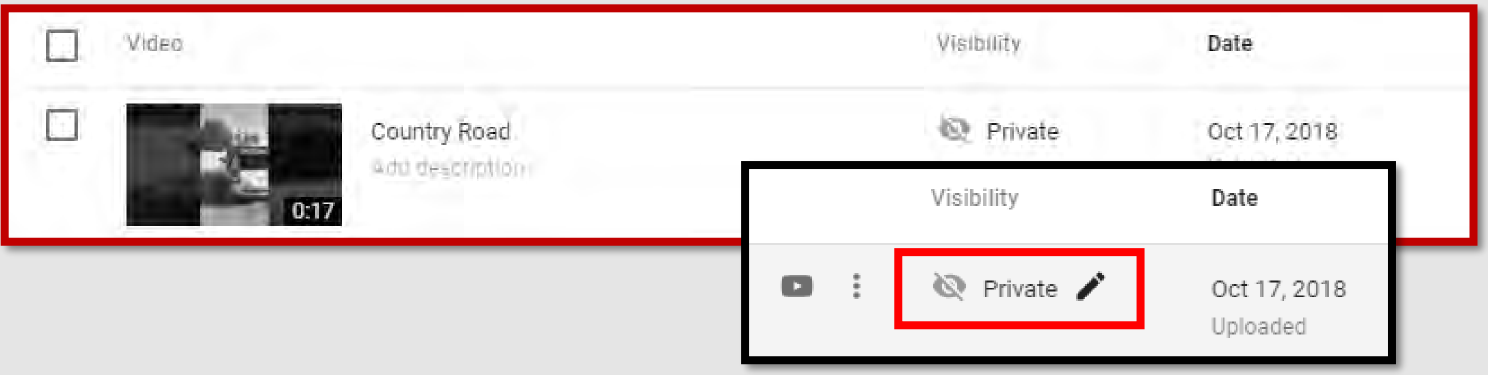
Who can see your videos?

One of the main uses for YouTube is of course uploading and watching videos. In order to upload your videos and create privacy settings you must first locate your "Video Manager." Select the "Google Profile" icon, and on the dropdown menu select "Your Channel." Then press the blue "Manage Videos" button. Here you will be able to upload and edit videos.

In order to edit the "Visibility" of a video, or who can see the video, simply hover over the "Visibility" column next to the video and select the "Down Arrow" or the "Edit" icon. From the popup menu that appears, you can choose "Private", "Unlisted", or "Public" - we recommend you select "Unlisted".







The "Unlisted" privacy setting on YouTube means that your video is only visible to viewers who have a link to the video. "Private" means only you can view the video. And "Public" means anyone can search for the video and view it, react to it, and comment on it. Once a video is uploaded to YouTube and made "Public" there is no real way to pull back the video - it can be shared, liked, and commented on, and you lose control of it.

UPDATED JAN 2021

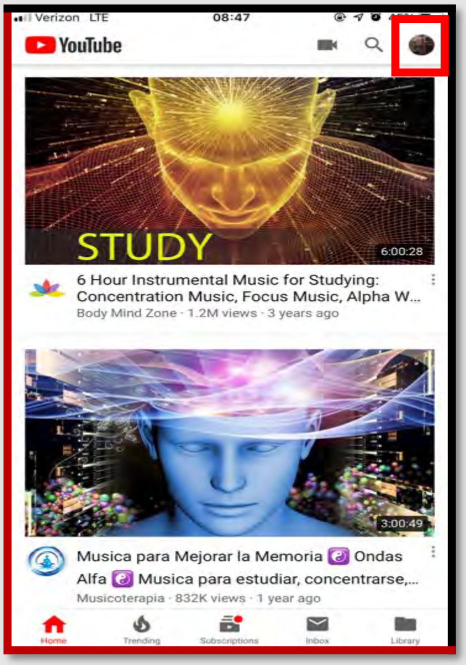
LOCKING DOWN YouTube

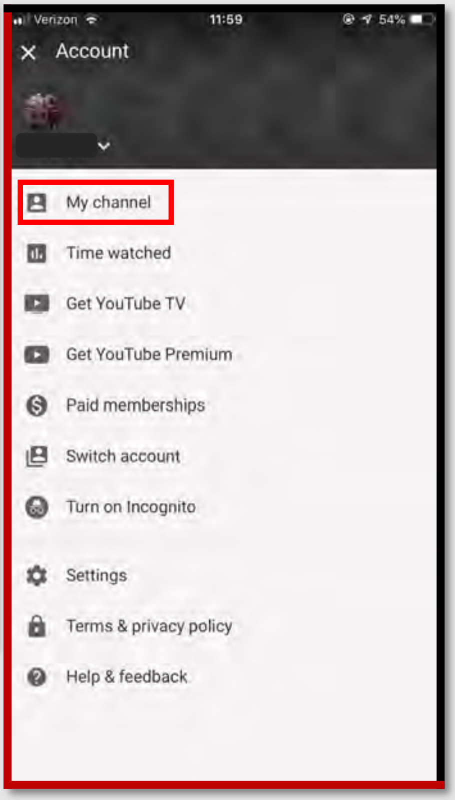
Mobile Device Version

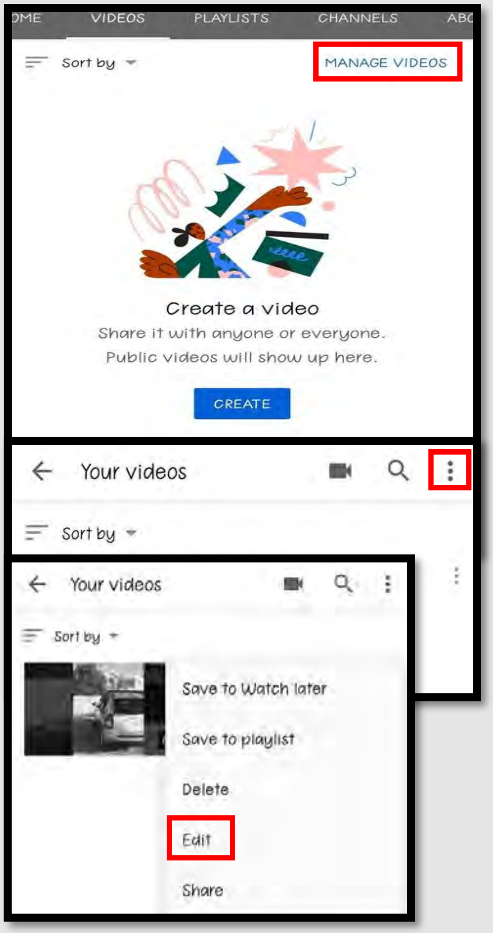
*** This information describes how to make your account secure on Android and iPhone mobile devices. Differences between iPhone Operating System (iOS) and Android Operating System (AOS) are minimal, in such cases iPhone images are outlined **black** and Android **red**.*

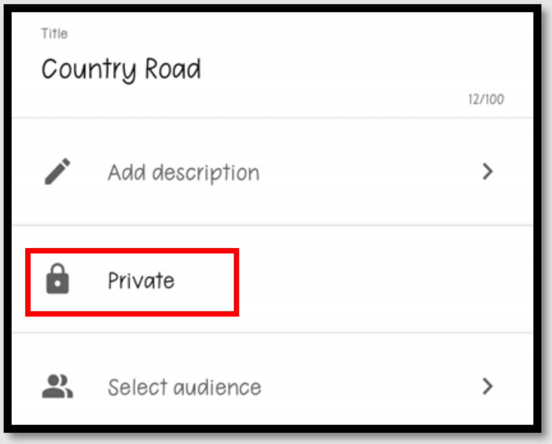
Unlike any other social networks, YouTube doesn't require you to create an account before you or your child can search for content or view videos.

Who can see your videos?


Verizon LTE
08:47
YouTube
STUDY
6:00:28
6 Hour Instrumental Music for Studying: Concentration Music, Focus Music, Alpha W...
Body Mind Zone · 1.2M views · 3 years ago
3:00:49
Musica para Mejorar la Memoria Ondas Alfa Musica para estudiar, concentrarse,...
Musicoterapia · 832K views · 1 year ago
Home
Trending
Subscriptions
Inbox
Library







In order to access uploaded videos and change their privacy settings via your smart devices, follow these steps.. From the "YouTube App", select your "Google Profile" picture / icon, then select "My Channel." Next head to the top menu and select "Videos" to take you to the video upload section. From there select "Manage Videos" from the upper right hand corner. The videos you have uploaded appear here, and you can edit them from this page by selecting the three ellipses to the right of each video, then select "Edit", and then select "Privacy" and choose your privacy setting - we recommend "Private" or "Unlisted".

The "Unlisted" privacy setting on YouTube means that your video is only visible to viewers who have a link to the video. "Private" means only you can view the video. And "Public" means anyone can search for the video and view it, react to it, and comment on it. Once a video is uploaded to YouTube and made "Public" there is no real way to pull back the video - it can be shared, liked, and commented on, and you lose control of it.

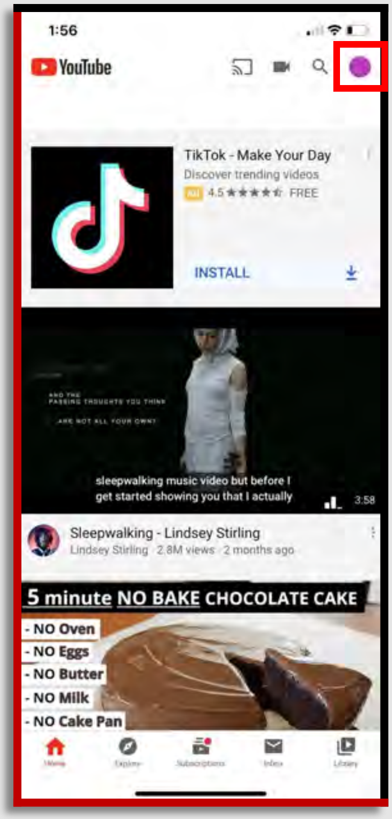
UPDATED JAN 2021

LOCKING DOWN YouTube

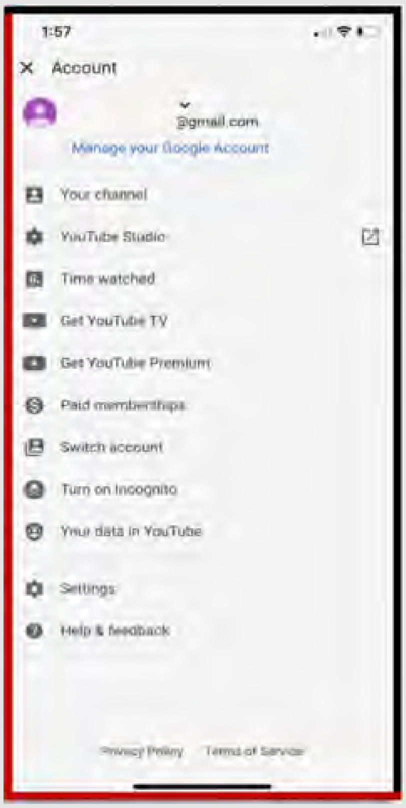
Mobile Device Version

*** This information describes how to make your account secure on Android and iPhone mobile devices. Differences between iPhone Operating System (iOS) and Android Operating System (AOS) are minimal, in such cases iPhone images are outlined **black** and Android **red**.*

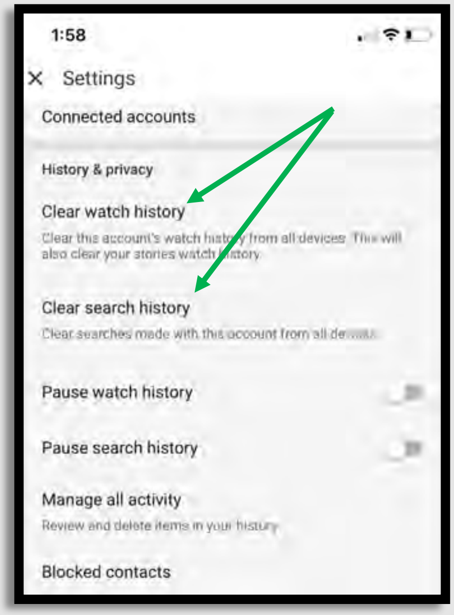
Clear History



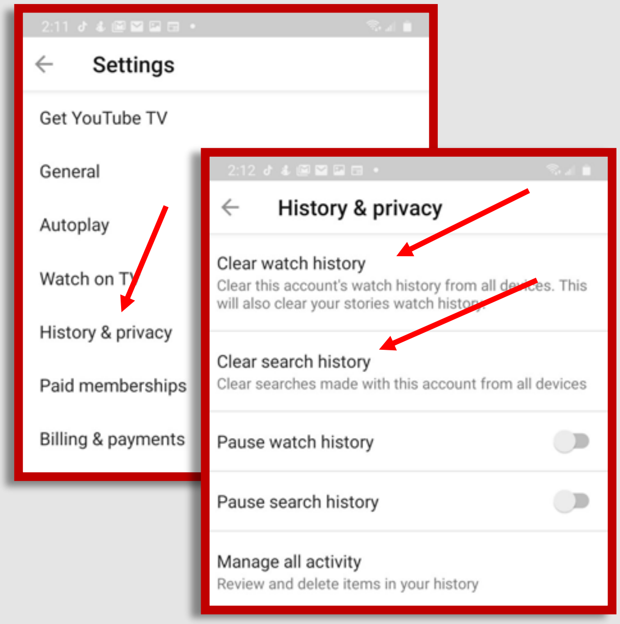
1:56
YouTube
TikTok - Make Your Day
Discover trending videos
4.5 ★★★★★ FREE
INSTALL
AND THE PASSING THOUGHTS YOU THINK ARE NOT ALL YOUR OWN
sleepwalking music video but before I get started showing you that I actually
3:58
Sleepwalking - Lindsey Stirling
Lindsey Stirling · 2.8M views · 2 months ago
5 minute NO BAKE CHOCOLATE CAKE
- NO Oven
- NO Eggs
- NO Butter
- NO Milk
- NO Cake Pan



1:57
✕ Account
@gmail.com
Manage your Google Account
Your channel
YouTube Studio
Time watched
Get YouTube TV
Get YouTube Premium
Paid memberships
Switch account
Turn on Incognito
Your data in YouTube
Settings
Help & feedback
Privacy Policy · Terms of Service



1:58
✕ Settings
Connected accounts
History & privacy
Clear watch history
Clear this account's watch history from all devices. This will also clear your stories watch history.
Clear search history
Clear searches made with this account from all devices
Pause watch history
Pause search history
Manage all activity
Review and delete items in your history
Blocked contacts



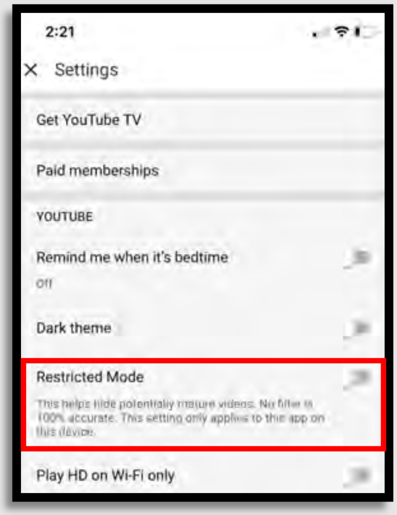
← Settings
Get YouTube TV
General
Autoplay
Watch on TV
History & privacy
Paid memberships
Billing & payments

← History & privacy
Clear watch history
Clear this account's watch history from all devices. This will also clear your stories watch history.
Clear search history
Clear searches made with this account from all devices
Pause watch history
Pause search history
Manage all activity
Review and delete items in your history

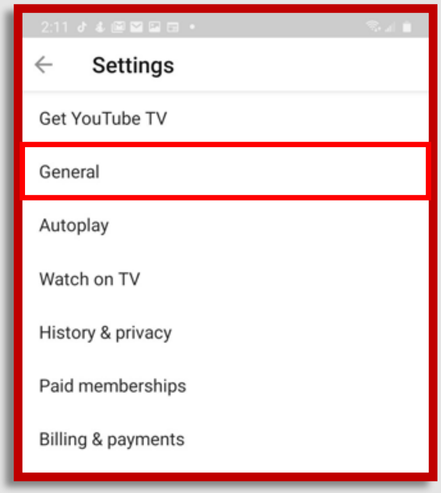
On iPhone (images outlined black): select your "Google Profile" icon, then select "Settings", scroll down to "History & Privacy". Follow prompts for "Clear watch history" and "Clear search history".

On Android (images outlined red): select your "Google Profile" icon, then select "Settings", then "History & privacy". Follow the prompts to "Clear watch history" and "Clear search history".

Restrict Mature Content



2:21
✕ Settings
Get YouTube TV
Paid memberships
YOUTUBE
Remind me when it's bedtime
Off
Dark theme
Restricted Mode
This helps hide potentially mature videos. No filter is 100% accurate. This setting only applies to this app on this device.
Play HD on Wi-Fi only



← Settings
Get YouTube TV
General
Autoplay
Watch on TV
History & privacy
Paid memberships
Billing & payments

On iPhone: go back to "Settings", then set the "Restricted Mode" toggle to "On"

On Android: under "Settings", select "General", scroll down to "Restricted Mode" and set the toggle to "On".

Remember this is a good idea if you have children that use your YouTube account.

Your phone is your ultimate endpoint. You likely carry it everywhere and it holds your most sensitive information. Make sure to check for updates quarterly. #Staysafeonline

UPDATED JAN 2021

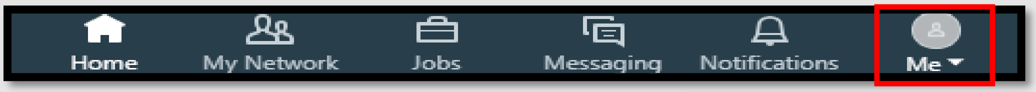
LINKEDIN SMART CARD

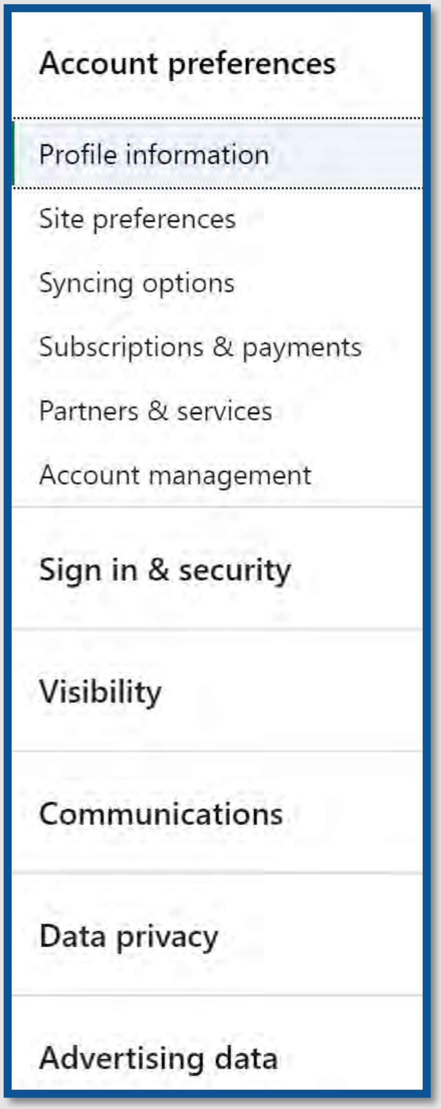
Personal Computer (PC) Version

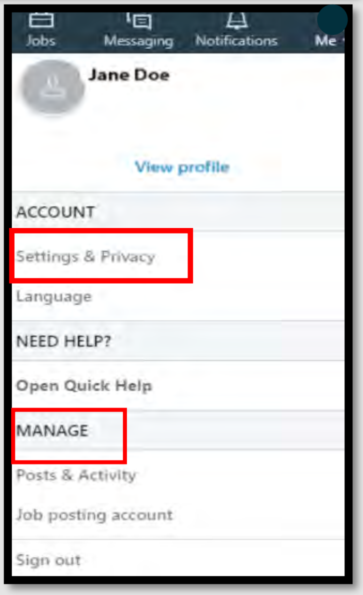
Do's and Don'ts

- ***Do not*** use an email account that is associated with your banking, finances, or other important contacts. Instead, consider creating an email account specific to this site.
- ***Do not*** establish connections with people you do not know and trust, not everyone is who they say they are.
- ***Do not*** register, log in, or link third party sites (e.g. Facebook, Twitter, etc.) using your LinkedIn account. Third party sites may aggregate and misuse your personal information and data.
- ***Do*** review your connections often to ensure that ensure they are current and that you are not providing your information to individuals who no longer need it.
- ***Do*** consider your profile picture. Posting a profile picture is optional, and we recommend that if you decide to post a picture, you dress in professional business attire.
- ***Do*** ensure that family members take similar precautions with their accounts. Their privacy and share settings can expose your personal data.

LinkedIn is the largest professional network on the Internet. It is used to find the right job, connect and strengthen professional networks, and learn professional skills. But a lot of sensitive personal information is uploaded to this site. See how to protect yours using the guidance below.







The "Settings" section for LinkedIn can be found in under the "Me" menu on the top right corner of the website (shown above). LinkedIn recently changed their "Settings" section, so it is a good idea to check and make sure your LinkedIn settings remained untouched and set to your standards. Later in this card we will discuss items from the "Manage" section of the drop down menu (to your right) so it is important to take note of its location. From the drop down menu, select "Settings & Privacy" (highlighted in **red** to the right). A new screen will appear with a header like the one shown to your left here. The first section we are going to review is the "Account Preferences" settings.

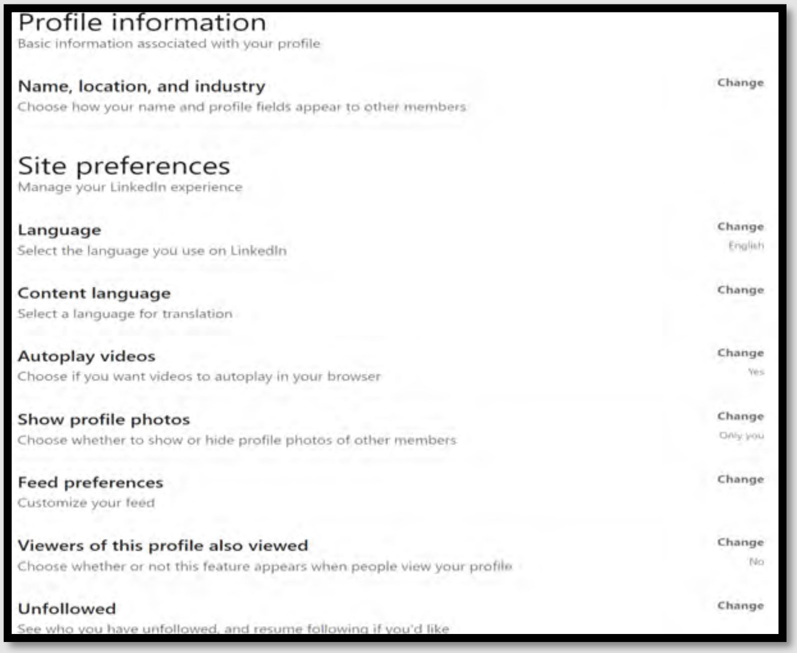
First, in the "Profile Information" menu, you can see basic LinkedIn personal information. In this section you can review any information that might be considered PII or that you may no longer want visible to other LinkedIn members. Remember that while LinkedIn can be a great tool for seeking employment, once you have obtained employment it is recommended that you limit the information that is visible to all LinkedIn members to ensure your privacy. Additionally, in this section (shown on the next page) LinkedIn gives you the option to provide a maiden name, however it is highly recommended that you do not provide such information as it is unnecessary to the immediate employment search and can be provided on an as needed basis later in the employment process.

Sign out of your accounts after you use a publicly shared computer or your home computer. #stophackers #keepyouraccountsafe

LINKEDIN SMART CARD

Personal Computer (PC) Version

Next look through the "Site Preferences: section and review and update all necessary settings. Here it is recommended that you update "Show profile photos" so that only "your connections" or "only you" can view your photo. It is also important when considering which photo to use on LinkedIn, that you use a photo that has a clean background, nothing in the background should give away any information that you would otherwise not want others to see or know. While you are utilizing LinkedIn for employment purposes it is likely that you will want to leave "on" the "Viewers of this profile also viewed" preference. However once you no longer need LinkedIn for employment purposes but instead purpose keep it as an updating tool, you may want to change this setting to "no."



Profile information
Basic information associated with your profile

Name, location, and industry — Change
Choose how your name and profile fields appear to other members

Site preferences
Manage your LinkedIn experience

Language — Change
Select the language you use on LinkedIn — English

Content language — Change
Select a language for translation

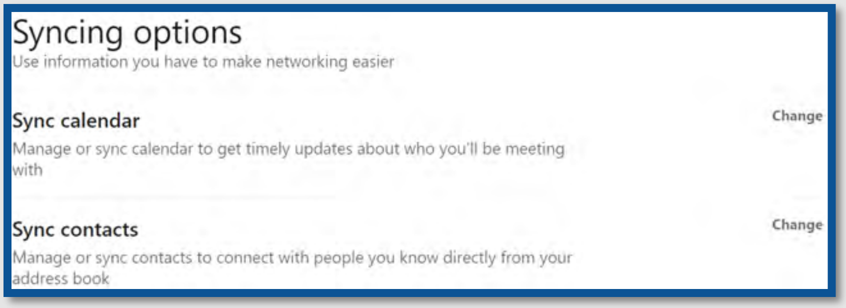
Autoplay videos — Change
Choose if you want videos to autoplay in your browser — Yes

Show profile photos — Change
Choose whether to show or hide profile photos of other members — Only you

Feed preferences — Change
Customize your feed

Viewers of this profile also viewed — Change
Choose whether or not this feature appears when people view your profile — No

Unfollowed — Change
See who you have unfollowed, and resume following if you'd like



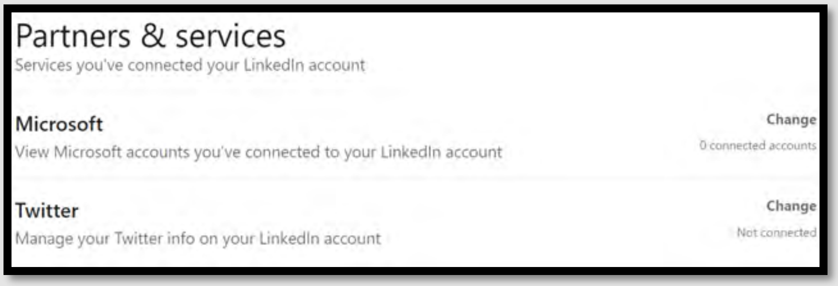
Syncing options
Use information you have to make networking easier

Sync calendar — Change
Manage or sync calendar to get timely updates about who you'll be meeting with

Sync contacts — Change
Manage or sync contacts to connect with people you know directly from your address book

Now look to the "Syncing options" section. Here LinkedIn gives you the option to link your calendar and/or contacts with LinkedIn. It is highly recommended that neither of these functions be used. Providing your calendar could inadvertently provide LinkedIn with PII of yours or of someone else's, as is the case with linking your contacts on the site.

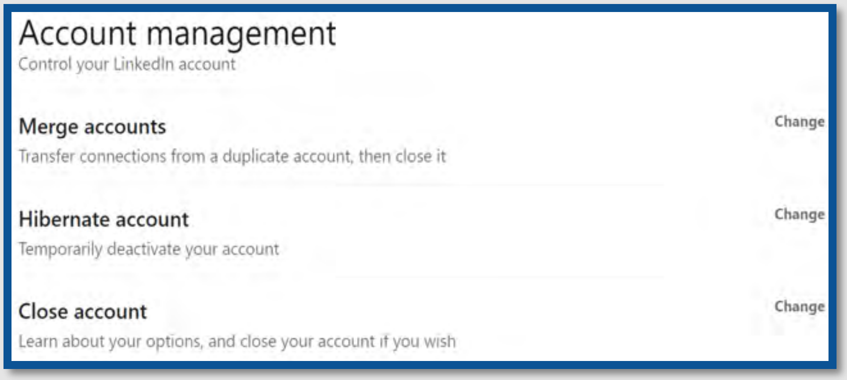
In the "Partners & Services" section, LinkedIn asks you to link your account with other accounts you may be signed up too such as Twitter. Much like the "Syncing options" preferences, this is not recommended as a safe option.



Partners & services
Services you've connected your LinkedIn account

Microsoft — Change
View Microsoft accounts you've connected to your LinkedIn account — 0 connected accounts

Twitter — Change
Manage your Twitter info on your LinkedIn account — Not connected



Account management
Control your LinkedIn account

Merge accounts — Change
Transfer connections from a duplicate account, then close it

Hibernate account — Change
Temporarily deactivate your account

Close account — Change
Learn about your options, and close your account if you wish

Finally, in "Account management" you are provided the option to "Merge accounts." If you have created new account because a malicious action occurred on your previous LinkedIn, it is not recommended that you blend the new account with the old account. Any malicious activity (especially if someone else has obtained access to the old account) will be merged onto your new account.

Manage your account information and privacy settings from your Settings & Privacy page. Remember to update update! #privacymatters.

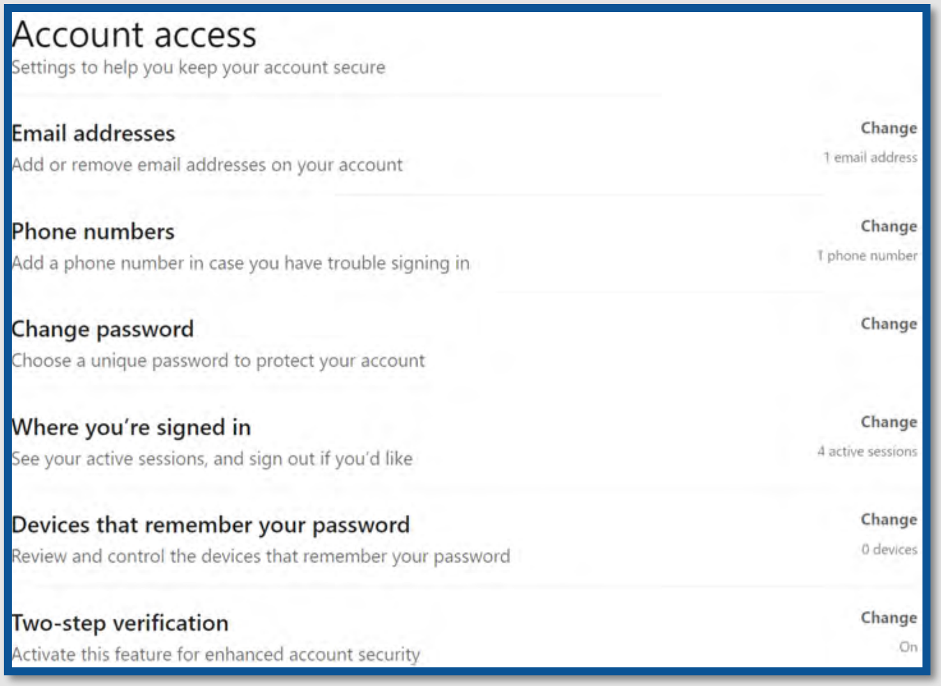
LINKEDIN SMART CARD

Personal Computer (PC) Version

Next select “Sign in & security” from the menu on the left hand side of your screen. Here you can review your user information i.e. what emails and phone numbers are associated with your account. This becomes especially important to know if you believe someone may have gained access to your account. One of the first things a hacker will do, aside from changing your password, is to change your email address so that you cannot regain access.

In this section you can also review “Where you’re signed in” which is another great tool to help you ensure that you are the only one with access to your account.

Most important to note in this section is the “Two-step verification” preference. It is important and highly recommended through the Smart Guide, that you enable this function. Likely, enabling this function will require a code from your smart device any time you log on from a location that is unfamiliar to the LinkedIn system.



Account access

Settings to help you keep your account secure

Email addresses — Add or remove email addresses on your account — Change — 1 email address

Phone numbers — Add a phone number in case you have trouble signing in — Change — 1 phone number

Change password — Choose a unique password to protect your account — Change

Where you’re signed in — See your active sessions, and sign out if you’d like — Change — 4 active sessions

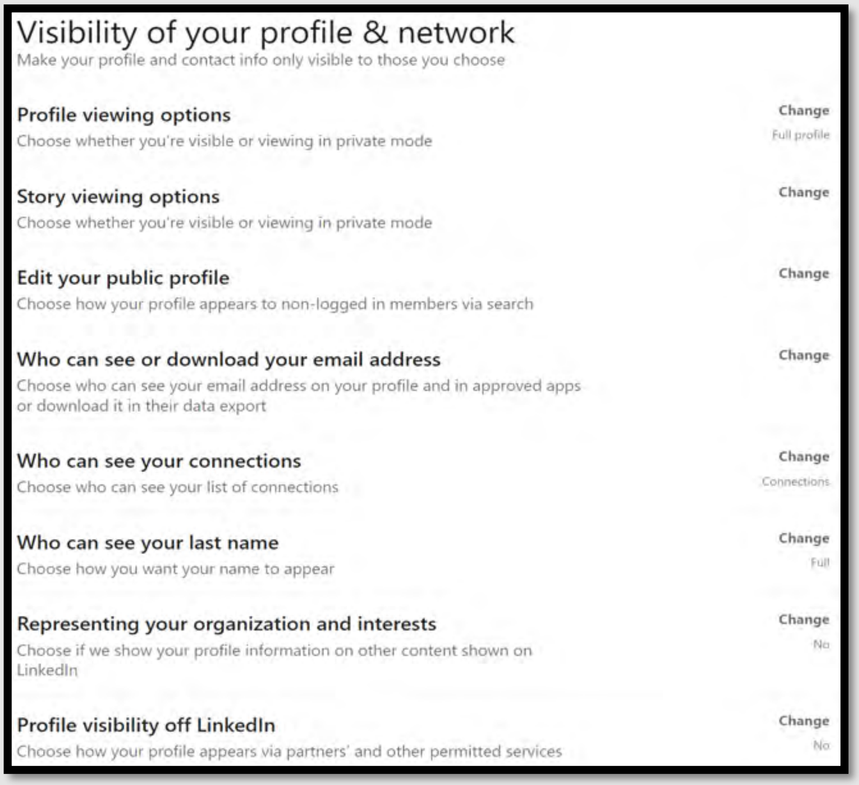
Devices that remember your password — Review and control the devices that remember your password — Change — 0 devices

Two-step verification — Activate this feature for enhanced account security — Change — On

Next, in the “Visibility” section (located on the right of your screen as seen on the first page of this card) we will begin with the “Profile viewing options.” This section refers to what others see when you view their profile. If you are seeking employment it might be beneficial to allow your “full profile” to be viewed, however once you have obtained employment it is important to go in and lock this feature down. The same applies to the “Story viewing options.”

Moving on to “Edit your public profile,” it is recommended that you not allow those who are not logged to LikedIn to view your profile. It is also recommended that you not allow any individual to download or see your email address or your connections. Allowing others to view your connections could allow users to obtain additional information about you that you would otherwise not have noted on your profile.

It is not recommended, whether searching for a job or not, that you allow LinkedIn to show you “Representing your organization and interests” It is uncertain whether or not you would even be aware that your profile was being used in these instances. The “Profile visibility off LinkedIn” preference allows you to deny LinkedIn the ability to show your profile information with services outside of LinkedIn such as Outlook. It is not recommended that you turn this function on.



Visibility of your profile & network

Make your profile and contact info only visible to those you choose

Profile viewing options — Choose whether you’re visible or viewing in private mode — Change — Full profile

Story viewing options — Choose whether you’re visible or viewing in private mode — Change

Edit your public profile — Choose how your profile appears to non-logged in members via search — Change

Who can see or download your email address — Choose who can see your email address on your profile and in approved apps or download it in their data export — Change

Who can see your connections — Choose who can see your list of connections — Change — Connections

Who can see your last name — Choose how you want your name to appear — Change — Full

Representing your organization and interests — Choose if we show your profile information on other content shown on LinkedIn — Change — No

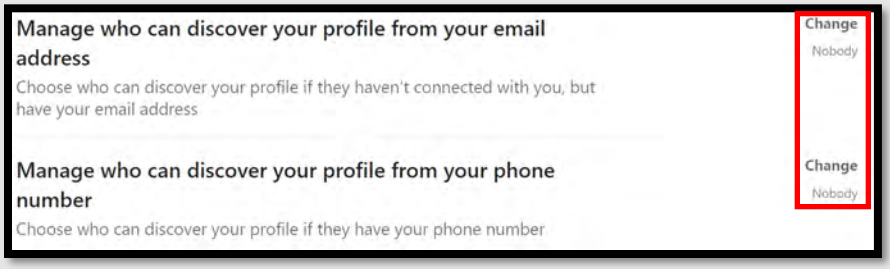
Profile visibility off LinkedIn — Choose how your profile appears via partners’ and other permitted services — Change — No

Be sure to verify accounts and users that are trying to connect with you on LinkedIn. If a company or user profile looks too empty it may be a fake account.

UPDATED JAN 2021

LINKEDIN SMART CARD

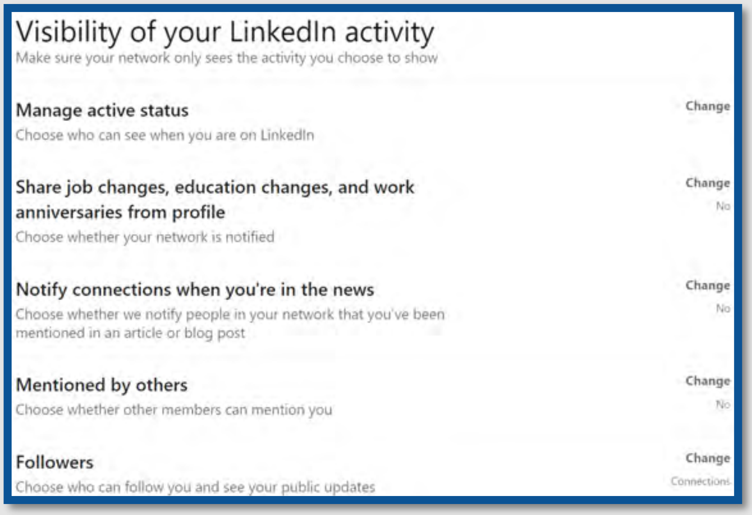
Personal Computer (PC) Version



Manage who can discover your profile from your email address
Choose who can discover your profile if they haven't connected with you, but have your email address
Change
Nobody

Manage who can discover your profile from your phone number
Choose who can discover your profile if they have your phone number
Change
Nobody

In the “manage who can discover your profile from your email address” and “manage who can discover your profile from your phone number” it is important to remember that employers may desire access to view your LinkedIn profile and therefore these functions may need to be “Everyone” or “2nd degree connections” depending on your link to the prospective company. However it is much safer to have these functions switched to “nobody” therefore once employment has been obtained it is recommended that you switch these functions to “Nobody.”



Visibility of your LinkedIn activity
Make sure your network only sees the activity you choose to show

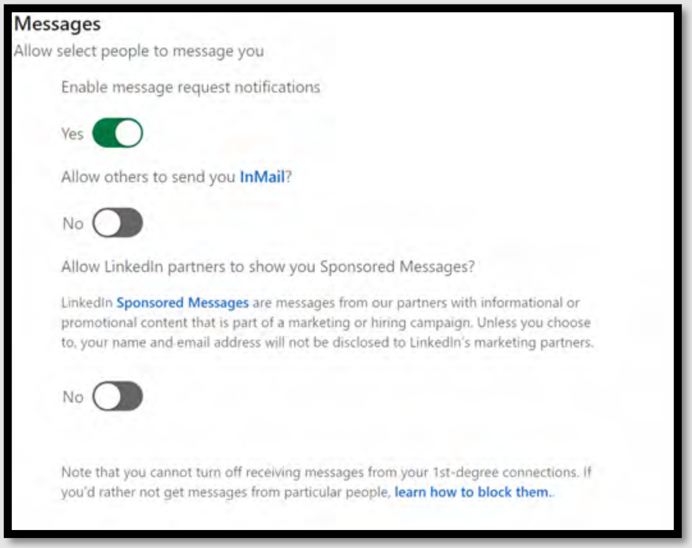
Manage active status
Choose who can see when you are on LinkedIn
Change

Share job changes, education changes, and work anniversaries from profile
Choose whether your network is notified
Change
No

Notify connections when you're in the news
Choose whether we notify people in your network that you've been mentioned in an article or blog post
Change
No

Mentioned by others
Choose whether other members can mention you
Change
No

Followers
Choose who can follow you and see your public updates
Change
Connections



Messages
Allow select people to message you

Enable message request notifications

Yes ●

Allow others to send you InMail?

No ○

Allow LinkedIn partners to show you Sponsored Messages?

LinkedIn Sponsored Messages are messages from our partners with informational or promotional content that is part of a marketing or hiring campaign. Unless you choose to, your name and email address will not be disclosed to LinkedIn's marketing partners.

No ○

Note that you cannot turn off receiving messages from your 1st-degree connections. If you'd rather not get messages from particular people, learn how to block them.

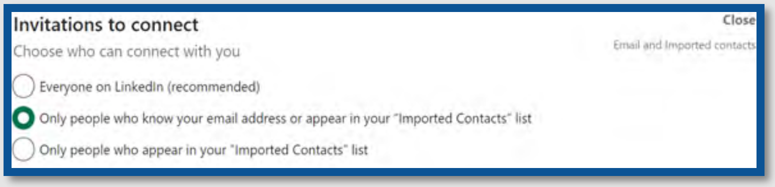
FYI - If you are a LinkedIn member but logged out of your account on a browser, LinkedIn may still continue to log your interaction with their services on that browser for up to 30 days. LinkedIn does this in order to generate usage analytics for their services, and they may share in aggregate form with their advertising customers.[1] #manageyourdata

Reference: 1. https://www.linkedin.com/legal/cookie-policy

Scrolling down to “Visibility of your LinkedIn activity” you will see several section that deal with notifying your connections of changes to your profile, mentions in news or even when you are active. If you used LinkedIn in order to search for and obtain employment and may not know personally all of your connections, then you may want to limit who can see updates that pertain to you and your lifestyle.

Here you can also decide whether or not other members can mention you in their post or otherwise. It is important to stay up to date on what content you are being mentioned in to ensure you agree with the information associated with your name.

Finally, you can decide who can follow you and view your public updates in this section. It is recommended that only your connections (with whom it is presumed you trust) can follow and see your public updates.



Invitations to connect
Choose who can connect with you
Close
Email and Imported contacts

○ Everyone on LinkedIn (recommended)
● Only people who know your email address or appear in your “Imported Contacts” list
○ Only people who appear in your “Imported Contacts” list

Lets look at the “Communications” section now, in order to do that simply select “Communications” from the left hand side of the screen. Many of the preferences here revolve around the type of notifications you receive from LinkedIn. However there are two settings here that need attention. The first is “Invitations to connect” (shown above). Here will can choose who can connect with you. Though it is not recommended that you import contacts to LinkedIn, LinkedIn gives the option of those who know your email OR appear in your “Imported Contacts List. This is the most recommended of the three options.

Lastly, you can determine who can message you in the “Messages” preference. It is recommended that you select “yes” to enable message request notifications, before allowing just anyone to message you.

Even LinkedIn recommends not putting your email address, home address, or phone number in your profile summary. #staysafeonline

UPDATED JAN 2021

LINKEDIN SMART CARD

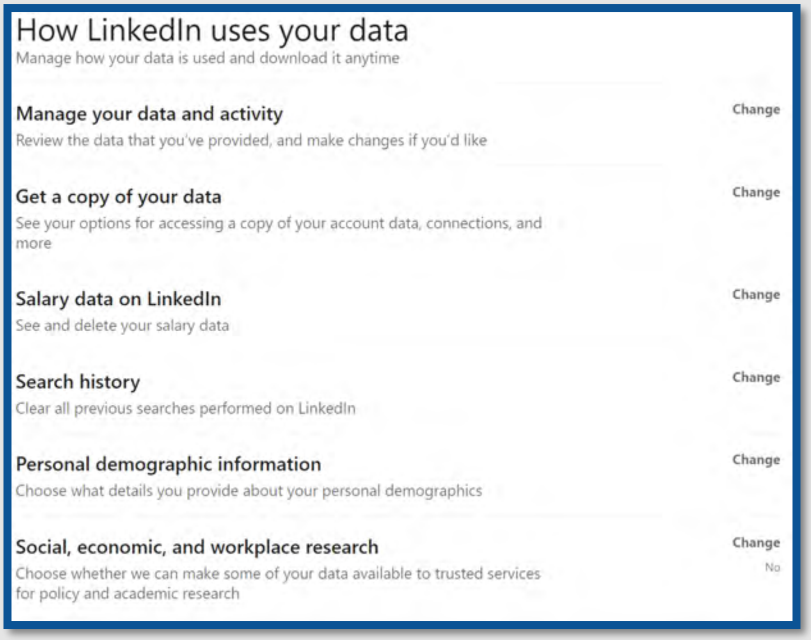
Personal Computer (PC) Version

Now let's look at the "Data privacy" section by selection it from the main menu located to the left of your screen.

Under "Mange your data and activity" you can review all changes made to your account since you joined LinkedIn. Much like Facebook's "Activity Log" it is a good idea to check here periodically to ensure you haven't been tagged or that you haven't yourself, put made changes that do not coincide with how you want others to preserve you or that might interfere with your privacy.

Under "Salary data on LinkedIn" it is recommended that you do not allow anyone to view your salary, this makes you more vulnerable to hacking and even home break ins.

Depending on what you are using LinkedIn for, it may be a good idea to allow LinkedIn to show your "Personal demographic information," however once you no longer need to display information such as that in this section it is recommended you go in and limit the type of information displayed about you. It is also not recommended that you enable the "Social, economic, and workplace research" preference and allow LinkedIn to share your data with any outside service.



How LinkedIn uses your data

Manage how your data is used and download it anytime

Manage your data and activity — Change

Review the data that you've provided, and make changes if you'd like

Get a copy of your data — Change

See your options for accessing a copy of your account data, connections, and more

Salary data on LinkedIn — Change

See and delete your salary data

Search history — Change

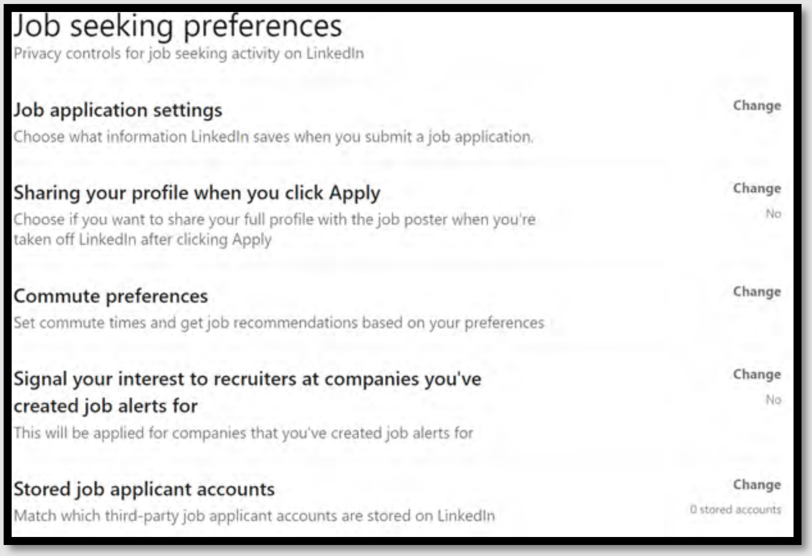
Clear all previous searches performed on LinkedIn

Personal demographic information — Change

Choose what details you provide about your personal demographics

Social, economic, and workplace research — Change — No

Choose whether we can make some of your data available to trusted services for policy and academic research



Job seeking preferences

Privacy controls for job seeking activity on LinkedIn

Job application settings — Change

Choose what information LinkedIn saves when you submit a job application.

Sharing your profile when you click Apply — Change — No

Choose if you want to share your full profile with the job poster when you're taken off LinkedIn after clicking Apply

Commute preferences — Change

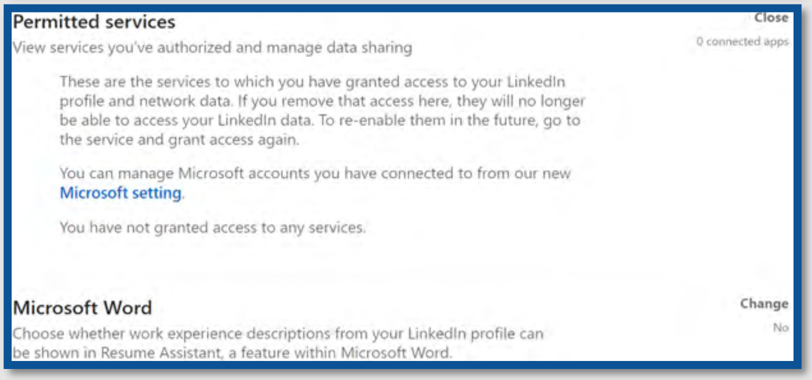
Set commute times and get job recommendations based on your preferences

Signal your interest to recruiters at companies you've created job alerts for — Change — No

This will be applied for companies that you've created job alerts for

Stored job applicant accounts — Change — 0 stored accounts

Match which third-party job applicant accounts are stored on LinkedIn



Permitted services — Close — 0 connected apps

View services you've authorized and manage data sharing

These are the services to which you have granted access to your LinkedIn profile and network data. If you remove that access here, they will no longer be able to access your LinkedIn data. To re-enable them in the future, go to the service and grant access again.

You can manage Microsoft accounts you have connected to from our new Microsoft setting.

You have not granted access to any services.

Microsoft Word — Change — No

Choose whether work experience descriptions from your LinkedIn profile can be shown in Resume Assistant, a feature within Microsoft Word.

Moving on to the "Job seeking preferences" where there are many sections here that require your attention. First, in "Job application settings" you will need to decide whether or not to allow LinkedIn to maintain copy of your resume, work experience and skills. It is recommended that you go directly to the company website to apply for employment instead of going through LinkedIn. It is recommended however, that if you do go through LinkedIn to apply for employment positions that once you obtain employment you remove your resume and any other additional information you shared with LinkedIn that you might not need on your account any longer.

In "Commute preferences" LinkedIn asks you to put your full address onto your profile (not for public view) so that they can accurately calculate your commute time. This is not recommended even while searching for employment.

Also, if you apply for jobs through LinkedIn it is a good idea to visit the "Stored job applicant accounts" preference periodically and remove any stored third party created accounts you may have unknowingly made when you applied for certain positions.

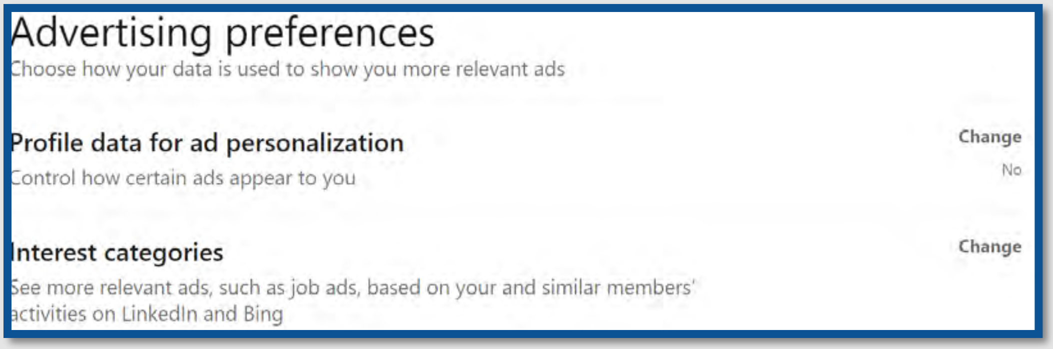
Finally, in "Other Applications" you will need to review the "Permitted services" and "Microsoft Word" preferences. In these section, again you can verify that you have not allowed LinkedIn to share any of your data with outside sources.

#PHISHINGALERT: Messages containing bad spelling, grammar, and that aren't addressed to you personally, or asking you to act immediately, are major red flags.

UPDATED JAN 2021

LINKEDIN SMART CARD

Personal Computer (PC) Version



Advertising preferences

Choose how your data is used to show you more relevant ads

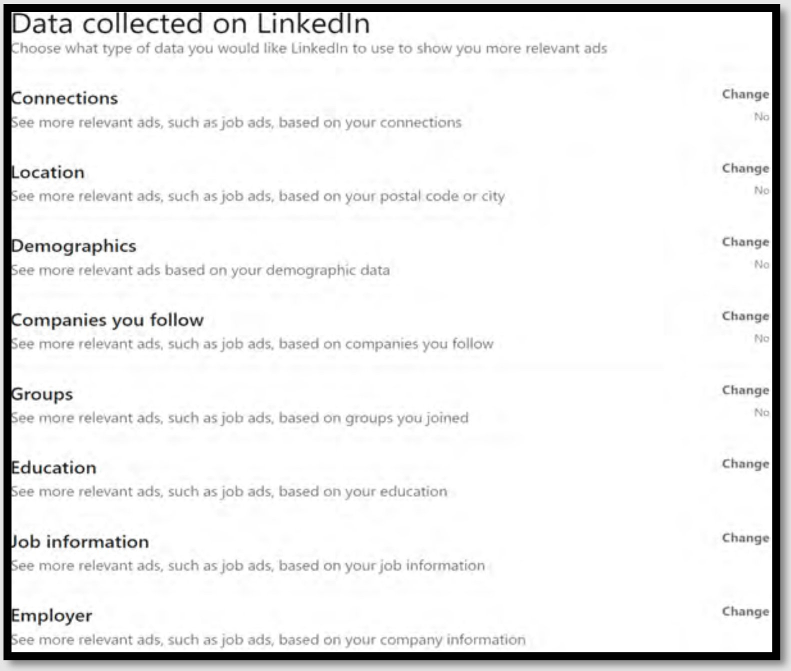
Profile data for ad personalization — Change — No

Control how certain ads appear to you

Interest categories — Change

See more relevant ads, such as job ads, based on your and similar members' activities on LinkedIn and Bing

In the final "Settings" section we will review the "Advertising preferences." Here it will be important to review each section to ensure you do not allow LinkedIn to use your data or photos for advertising purposes. First, in "Profile data for ad personalization" it is recommended this preference remain "no" so that you do not allow LinkedIn to use your photos or information to personalize ads for you. "Interest categories" allows LinkedIn to personalize ads and job postings based on items you may have clicked on or your profile information. It is not recommended that you turn this function on.



Data collected on LinkedIn

Choose what type of data you would like LinkedIn to use to show you more relevant ads

Connections — Change — No

See more relevant ads, such as job ads, based on your connections

Location — Change — No

See more relevant ads, such as job ads, based on your postal code or city

Demographics — Change — No

See more relevant ads based on your demographic data

Companies you follow — Change — No

See more relevant ads, such as job ads, based on companies you follow

Groups — Change — No

See more relevant ads, such as job ads, based on groups you joined

Education — Change

See more relevant ads, such as job ads, based on your education

Job information — Change

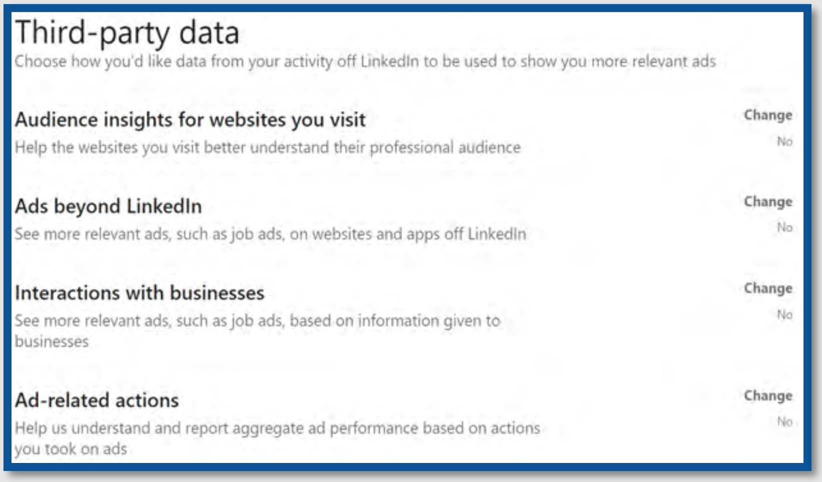
See more relevant ads, such as job ads, based on your job information

Employer — Change

See more relevant ads, such as job ads, based on your company information

Moving on, let's review "Data collected on LinkedIn" preferences. Here is yet another location where LinkedIn attempts to use your profile information in order to create and show you (and others) more personalized ads to include job ads. The use of information is broken down in this section by subsections or individual preferences, where you will need to go in and select "no" for each one in order to deny LinkedIn the capability to use your information. Under "Education," "Job information," and "Employer" you will need to go in and select or unselect each category as there are multiple.

Finally, under "Third-party data" (see below) you will want to review each preference as they all relate to sharing your data on sites other than LinkedIn or from other sites into LinkedIn. It is recommended that you not allow LinkedIn to push or pull any information about you, enable "no" under each sub preference in this category to decrease your personal information from being shared.



Third-party data

Choose how you'd like data from your activity off LinkedIn to be used to show you more relevant ads

Audience insights for websites you visit — Change — No

Help the websites you visit better understand their professional audience

Ads beyond LinkedIn — Change — No

See more relevant ads, such as job ads, on websites and apps off LinkedIn

Interactions with businesses — Change — No

See more relevant ads, such as job ads, based on information given to businesses

Ad-related actions — Change — No

Help us understand and report aggregate ad performance based on actions you took on ads

#PHISHINGALERT: Messages containing bad spelling, grammar, and that aren't addressed to you personally, or asking you to act immediately, are major red flags.

LINKEDIN SMART CARD

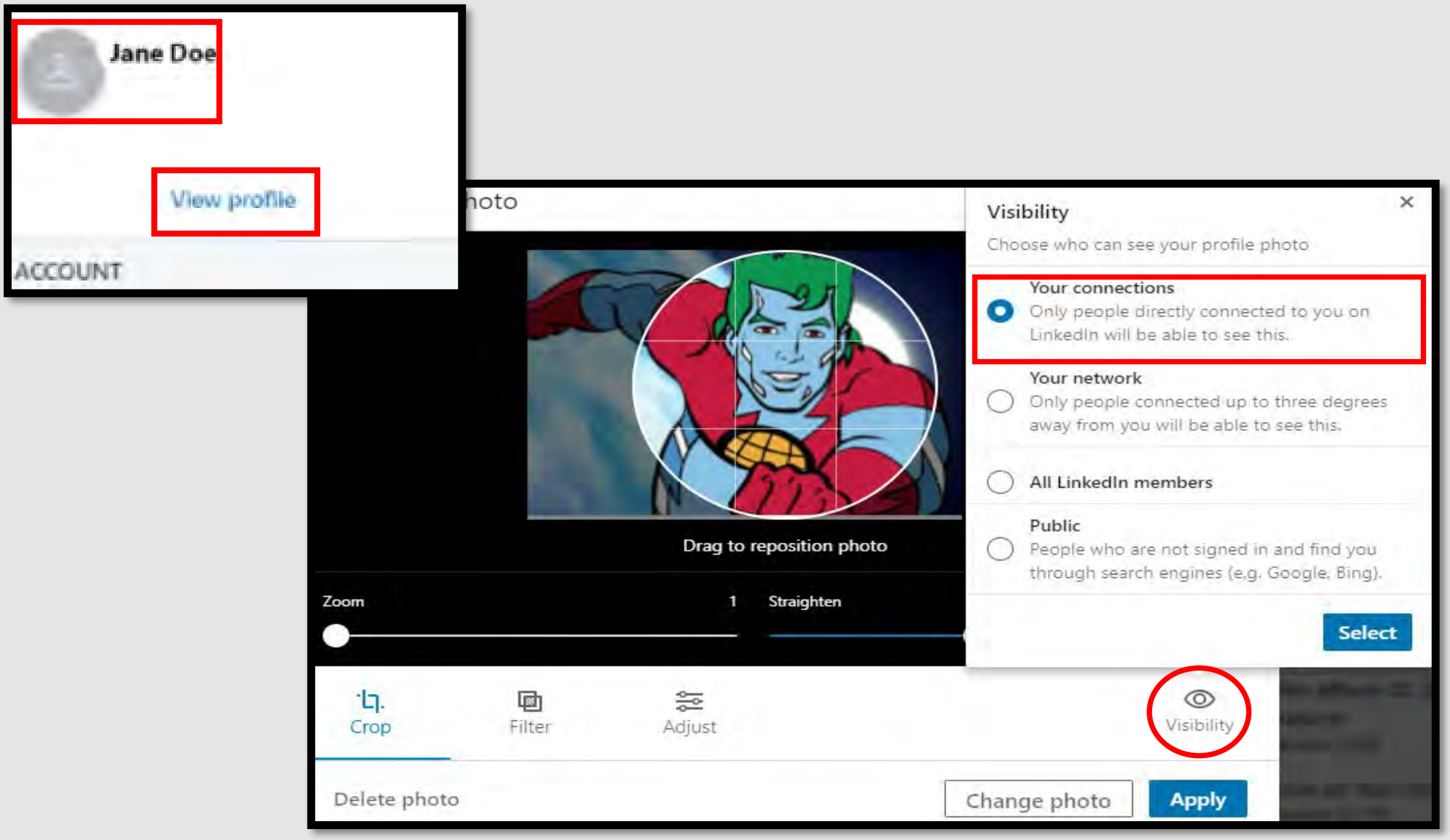
Personal Computer (PC) Version

Profile Picture

In addition to the “Security and Privacy” settings, it is important to look at your LinkedIn “Profile” and consider what kinds of information it is divulging about you. We recommend keeping profile data as general as possible, while still allowing it to serve your purposes for the account.

We recommend that you do ***not*** use photos of yourself for your profile or header photo. These are viewable to the public and so present an unnecessary vulnerability. If you decide to upload a profile picture, ensure that it is visible only to your “Connections”. Try to hide any obvious identifying marks that could make you more easily identified on anther website or in person.

To check your “Profiles” visibility to others, simply select the picture icon (see below highlighted in red) then again select your picture icon at which time a window will pop up. From there select “Visibility” located at the lower right of the pop up box. From here you can choose which category best fits your privacy needs. It is recommended that you select “Your connections” for visibility here, however if you are seeking employment it might be necessary to allow a much broader audience for some time. Just remember once you have gained employment to reset your privacy settings throughout LinkedIn.



Visibility ×

Choose who can see your profile photo

● Your connections
Only people directly connected to you on LinkedIn will be able to see this.

○ Your network
Only people connected up to three degrees away from you will be able to see this.

○ All LinkedIn members

○ Public
People who are not signed in and find you through search engines (e.g. Google, Bing).

Select

Stop. Think. Act - If anyone (a “Connection” or not) sends you a message with an attachment, will you open it? Does your action depend on whether or not you know and trust the sender? Even if someone you know sends you an attachment, it is a good idea to verify with that person over the phone or face-to-face that they are the sender before opening it. You may not know immediately if you’ve been hacked, and by the time you find out, it could be too late.

Private mode with a basic LinkedIn account will not allow you to see other users who have viewed your profile. #knowwhatyoudon’tknow

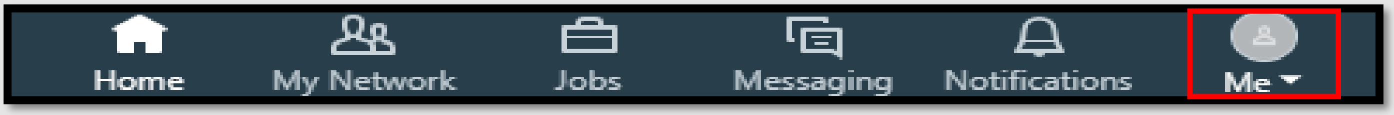
UPDATED JAN 2021

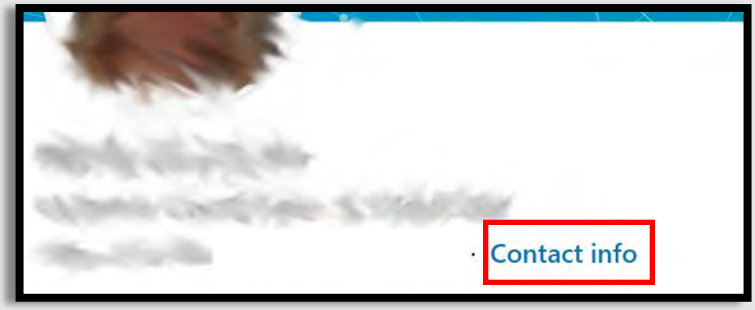
LINKEDIN SMART CARD

Personal Computer (PC) Version

https://www.linkedin.com/help/linkedin will provide you with additional and continuously up to date information on how LinkedIn is changing.

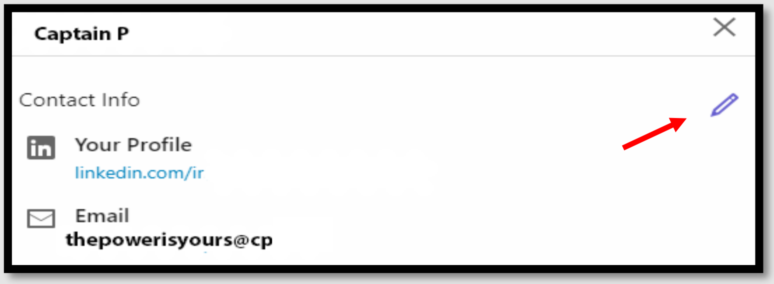
Date of Birth & Contact Info





To further protect your information you will need to check whether your “Date of Birth,” “Phone Number,” and “Email” are displayed on your profile page. In order to do this, click the “Me” tab at the top right of the page (usually with your picture in it), then select the “View Profile” link. This will take you to your “Profile” page.

On your “Profile” page, locate the “Contact Info” function, as shown above. Select the “Edit” or “Pencil” icon located to the upper right of the window. From there review the information shown and edit as necessary. Keep in mind that this is information that appears on your profile for others to see.



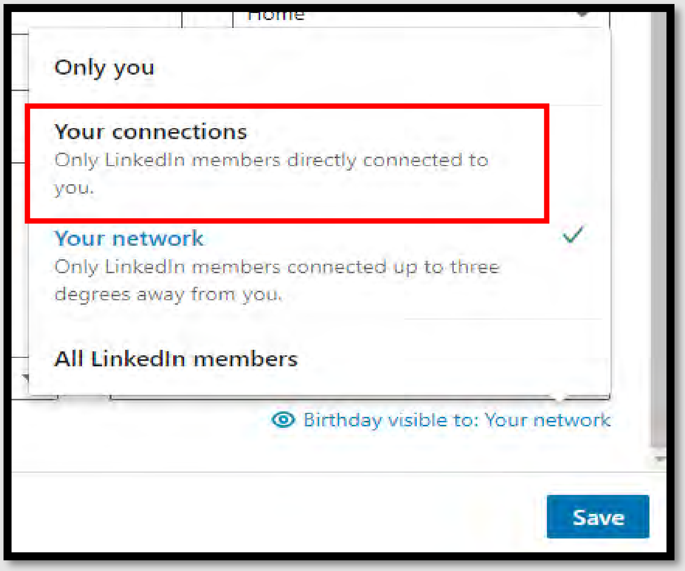
Captain P

Contact Info

Your Profile
linkedin.com/ir

Email
thepowerisyours@cp

We recommend you do ***not*** add a phone number, birthdate, or address in this section, and they are not required. LinkedIn requires an opt out of such information at multiple different stages throughout your profile. It is important to make sure you navigate through each one to ensure your privacy is set to your standards.


Home
Only you
Your connections
Only LinkedIn members directly connected to you.
Your network
Only LinkedIn members connected up to three degrees away from you.
All LinkedIn members
Save

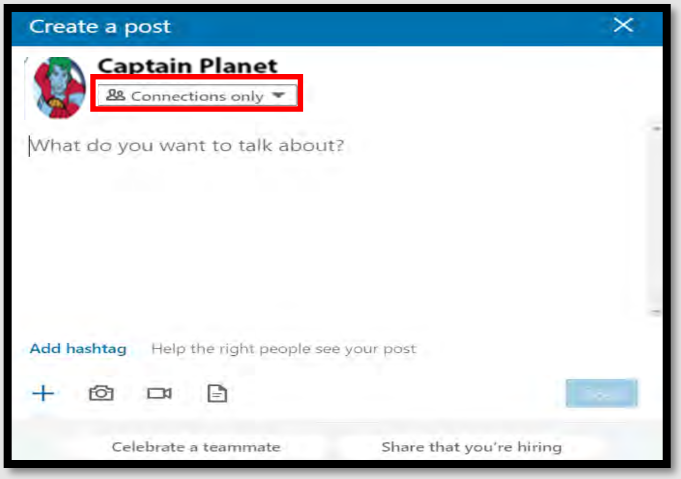
Birthday visible to: Your network

If it is important to you to display any of the above mentioned information, ensure that it is only visible to “Your Connections”. Do this by selecting the “Birthday visible to” link at the bottom of the screen (shown here to the left highlighted in **red**). Ensure that “Only you” or “Your Connections” is selected. Select the “Save” button before you exit out of this screen to keep selected settings.

Creating and Managing Posts

If you decide to create a post on LinkedIn, be sure to set the privacy settings of the posts containing personal information so those posts do not appear to the public. As shown in the box to the right, posts made “Public” on LinkedIn can be viewed by anyone.

In order to change the privacy settings for your post, simply locate the “Post Settings” drop down menu located on the post itself (highlighted right in **red**). From there select the appropriate audience for your post, we recommend “Connections only”.



Connections only

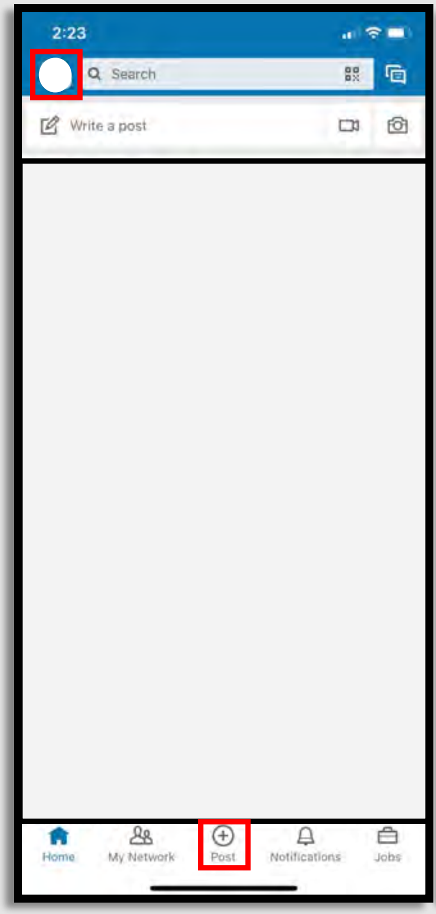
UPDATED JAN 2021

LINKEDIN SMART CARD

Mobile Device Version

*** This information describes how to make your account secure on Android and iPhone mobile devices. Differences between iPhone Operating System (iOS) and Android Operating System (AOS) are minimal, in such cases iPhone images are outlined **black** and Android **blue**.*

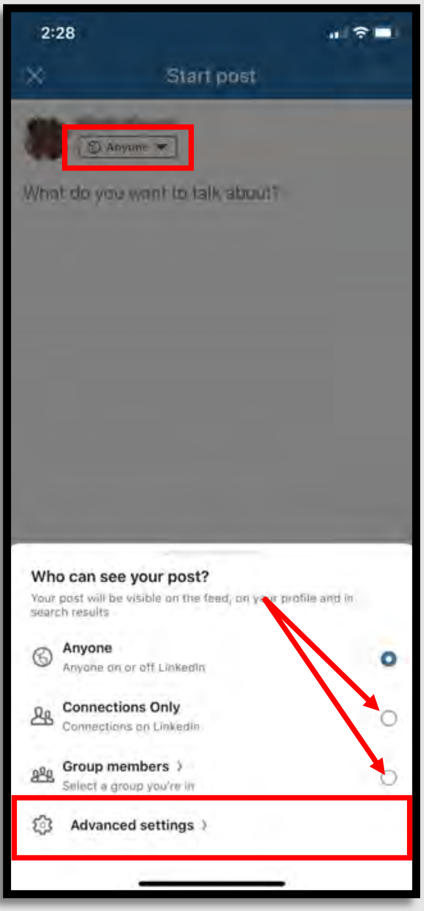
On iPhone: Select "Post" at the bottom center of the screen, then under your name select "Anyone", or the default. From the pop-up menu, select who you want to be able to see your post - we recommend "Connections only" or "Group members". You can also select "Advanced Settings" to "Disable comments on the post".



2:23

Search

Write a post



2:28

Start post

Anyone

What do you want to talk about?

Who can see your post?

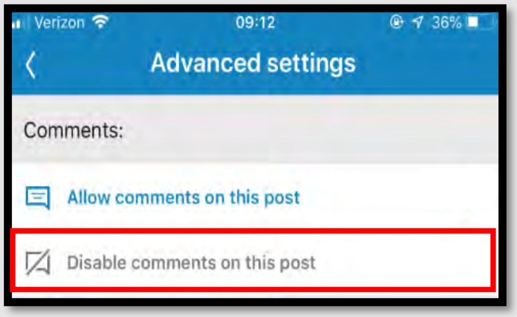
Your post will be visible on the feed, on your profile and in search results

● Anyone — Anyone on or off LinkedIn

○ Connections Only — Connections on LinkedIn

○ Group members › — Select a group you're in

Advanced settings ›



Verizon 09:12 36%

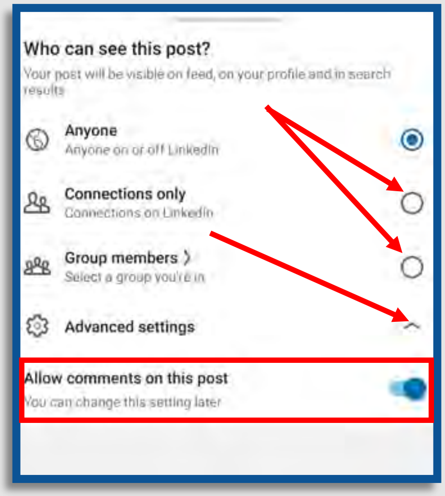
Advanced settings

Comments:

Allow comments on this post

Disable comments on this post

On Android: the process of locking down who can see your posts on Android is the same as on iPhone, except the "Advanced Settings". When you select "Advanced Settings", you will set the toggle to "Off" in order to disable comments for your post. (see below)



Who can see this post?

Your post will be visible on feed, on your profile and in search results

● Anyone — Anyone on or off LinkedIn

○ Connections only — Connections on LinkedIn

○ Group members › — Select a group you're in

Advanced settings

Allow comments on this post — You can change this setting later

Helpful Extra Hints

iOS/Android

To access your "**Privacy Settings**" page from your mobile device simply follow these steps:

1. Tap your "Profile" picture.

2. Tap the "Settings" function located under your name.

3. Navigate through the four tabs to adjust settings for "Account", "Privacy"," Ads", or "Communications".

Removing a mention

To remove a mention from a post or comment:

Click the **More** icon in the top right corner of a connection's post.
Click **Remove mention** from the list of options that appears.
Click **Remove**.

The post will no longer link to your profile. Once you've removed the mention, your name will still appear in plain text but the link to your profile won't be present.

Removing a tag

To remove a tag from a photo:

Click on the **Tag** icon on the photo.
Click on the **X** icon next to the tag with your name to remove the tag.

The member that mentioned you originally won't be notified that you've untagged yourself from the post.

To strengthen your password, try substituting numbers for letters that look similar. For example, substitute "0" for "o" or "3" for "E". #updateyourpassword

UPDATED JAN 2021

PLAYSTATION SMART CARD

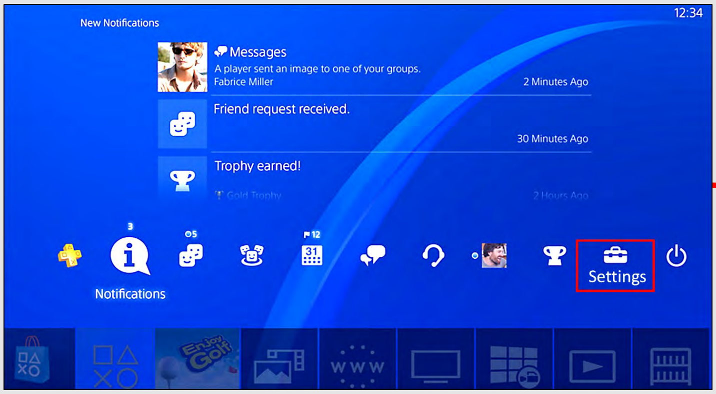
PS4

PlayStation's two-factor authentication is an added layer of security to ensure only authorized individuals have access to the system , accounts, and privacy information.

Do's and Don'ts

- ***Do*** use caution when sharing Gameplay when messages, video, audio, and personal data may be available to other users participating in your game experience.
- ***Do*** select "Friends Only" for all available settings options. Ensure family members take similar precautions with their accounts. Their privacy and share settings can expose your personal data.
- ***Do*** use parental controls to restrict access to questionable content and features for children using the PS4.
- ***Do*** refer to privacy policies / user agreements of individual games and third party applications to see if they use the PS4 camera, and to understand other privacy information.
- ***Don't*** forget to update your PS4 system to the latest version of the system software.
- ***Don't*** use pictures of yourself for your profile photos. Instead, use avatars or photos of something else. Profile photos are potentially viewable to other users and the public depending on your privacy settings.
- ***Don't*** discard or transfer ownership of your PlayStation without using "Initialization". Initialization sets your PS4 back to factory mode and erases the system data.
- ***Don't*** establish connections with individuals you do not know and trust. Understand that not everyone is who they say they are.

PlayStation allows you to manage a host of settings in order to take ownership of your system security and privacy, and determine what information other users can see. You must first access the "Settings" button from the "Dashboard Menu", highlighted below in red. From there, go to "Account Management".

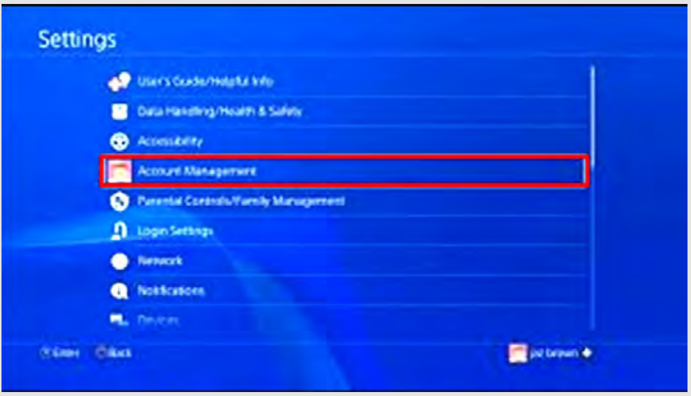

12:34

New Notifications

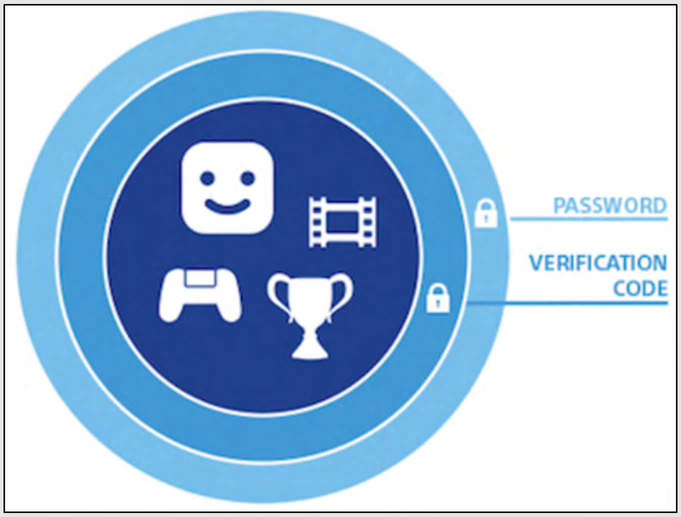
Messages
A player sent an image to one of your groups.
Fabrice Miller — 2 Minutes Ago

Friend request received. — 30 Minutes Ago

Trophy earned!
Gold Trophy — 2 Hours Ago


Settings
User's Guide/Helpful Info
Data Handling/Health & Safety
Accessibility
Account Management
Parental Controls/Family Management
Login Settings
Network
Notifications
Devices
Enter
Back

Two-Factor Authentication: To enhance the security of your PlayStation, we recommend you set up two-factor verification. Follow the detailed steps below, along with the graphical depiction of the steps on page two. From the "Account Management" screen, select "Account Information". Click on "Security". Next go to "2-Step Verification". Select "Set Up Now". Enter the phone number you want to set up to your account. A code will be sent to your mobile device. Verify your identity by entering the code sent to your mobile phone. This verifies you entered your phone number correctly. "Activate" the two-factor authentication. This adds an extra step to your basic log-in procedure, but can significantly help protect your system from being compromised later.



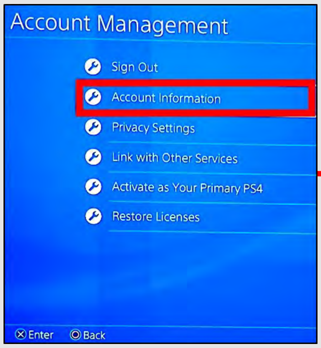
UPDATED JAN 2021

PLAYSTATION SMART CARD

PS4

It is good to understand PlayStation's privacy policies; however, users grant third party applications access to privacy information and these apps that have their own privacy policies.

2-Step Verification Graphics


Account Management

Sign Out

Account Information

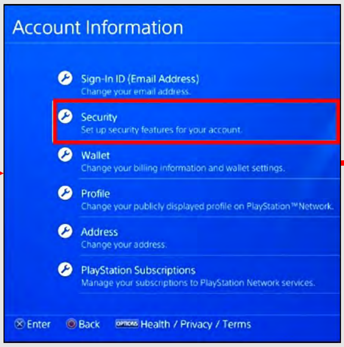
Privacy Settings

Link with Other Services

Activate as Your Primary PS4

Restore Licenses

Enter Back


Account Information

Sign-In ID (Email Address)
Change your email address.

Security
Set up security features for your account.

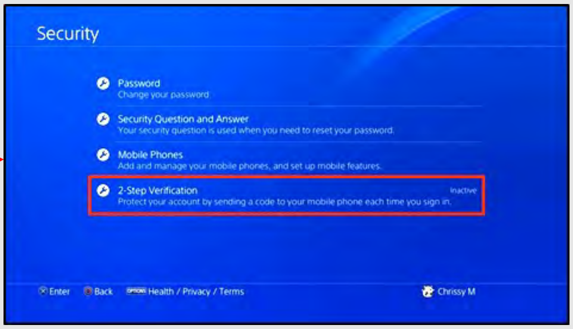
Wallet
Change your billing information and wallet settings.

Profile
Change your publicly displayed profile on PlayStation™Network.

Address
Change your address.

PlayStation Subscriptions
Manage your subscriptions to PlayStation Network services.

Enter Back OPTIONS Health / Privacy / Terms


Security

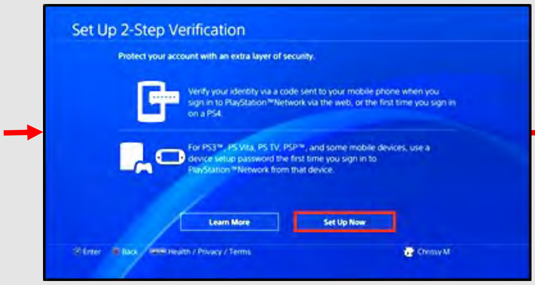
Password
Change your password.

Security Question and Answer
Your security question is used when you need to reset your password.

Mobile Phones
Add and manage your mobile phones, and set up mobile features.

2-Step Verification Inactive
Protect your account by sending a code to your mobile phone each time you sign in.

Enter Back OPTIONS Health / Privacy / Terms Chrissy M


Set Up 2-Step Verification

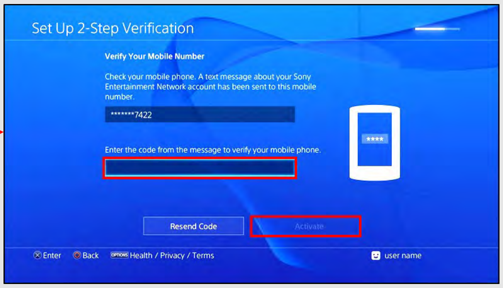
Protect your account with an extra layer of security.

Verify your identity via a code sent to your mobile phone when you sign in to PlayStation™Network via the web, or the first time you sign in on a PS4.

For PS3™, PS Vita, PS TV, PSP™, and some mobile devices, use a device setup password the first time you sign in to PlayStation™Network from that device.

Learn More Set Up Now

Enter Back OPTIONS Health / Privacy / Terms Chrissy M


Set Up 2-Step Verification

Verify Your Mobile Number

Check your mobile phone. A text message about your Sony Entertainment Network account has been sent to this mobile number.

*******7422

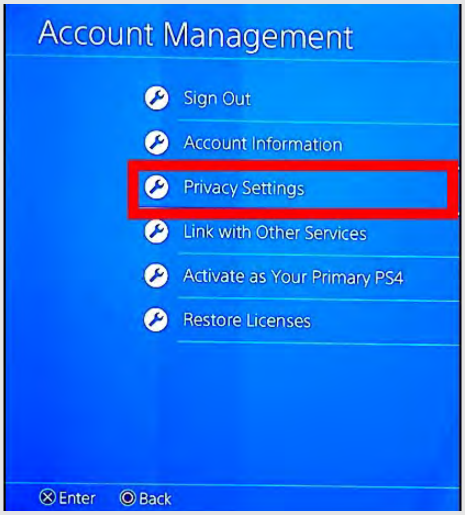
Enter the code from the message to verify your mobile phone.

Resend Code Activate

Enter Back OPTIONS Health / Privacy / Terms user name

Privacy Settings

Next, let's take a look at privacy settings. From the "Account Management" screen, select "Privacy Settings" as seen on the right highlighted in red. The "Gaming | Media" subcategory allows you to determine which activities are viewable by others. The "Friends | Connections" subcategory allows you to decide which status of individuals (e.g. friends, followers, etc) can view established connections. The "Personal Info | Messaging" subcategory allows you to choose who can see your real name and who can communicate with you. View the picture on the bottom right to see the privacy setting subcategories.


Account Management

Sign Out

Account Information

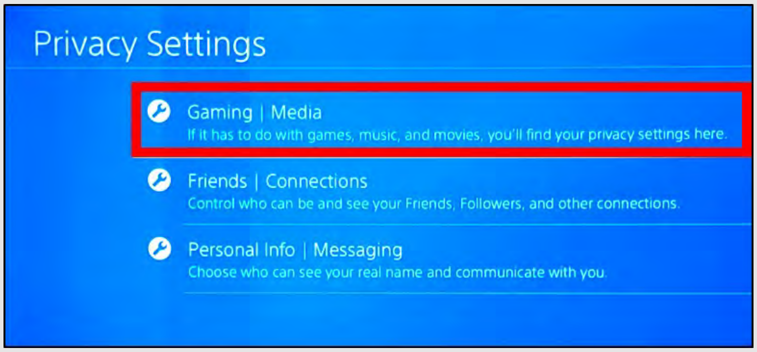
Privacy Settings

Link with Other Services

Activate as Your Primary PS4

Restore Licenses

Enter Back


Privacy Settings

Gaming | Media
If it has to do with games, music, and movies, you'll find your privacy settings here.

Friends | Connections
Control who can be and see your Friends, Followers, and other connections.

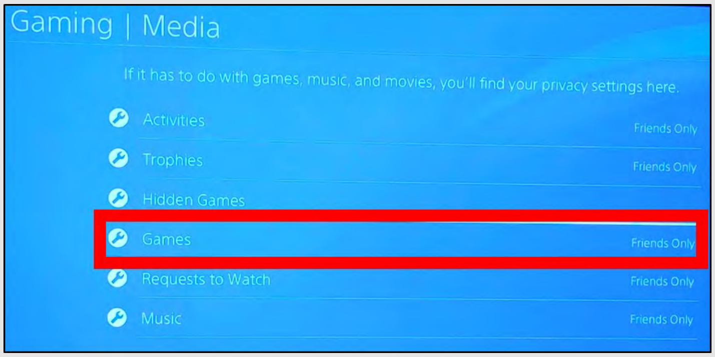
Personal Info | Messaging
Choose who can see your real name and communicate with you.

UPDATED JAN 2021

PLAYSTATION SMART CARD

Privacy Setting Recommendations

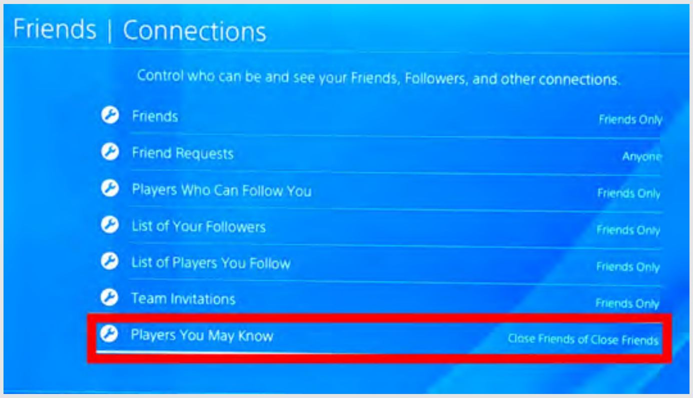
We recommend that you set your privacy settings to "Friends Only" for most sections, in order to prevent the general public from seeing information pertaining to the user. See "Recommended Privacy Settings" on the privacy settings graphics for "Gaming | Media", "Friends | Connections", and the "Personal Info | Messaging" subcategories. We recommend the primary user and family members be mindful of who they become friends with and connect to on the system. It is important to remember not everyone on your family and friends "Friends List," should be trusted. Parents, it is important to know not all users have good intentions, and are accurately portraying themselves online. For this reason, we recommend that you review your child's "friends" periodically. Other users on the system may utilize gaming systems to connect with potential victims or use social engineering against other users. If you do not know someone, we recommend you ***not*** add them to your "Friends List".



Gaming | Media

If it has to do with games, music, and movies, you'll find your privacy settings here.

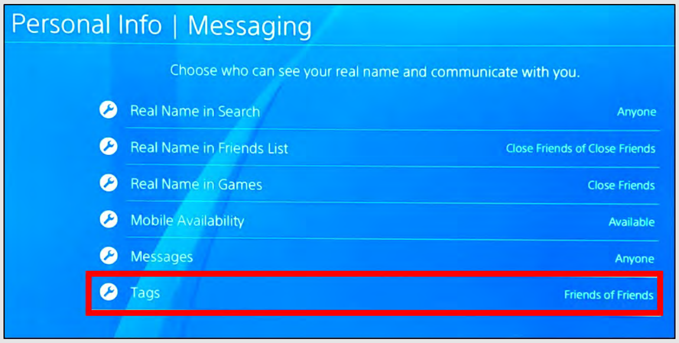
Activities	Friends Only
Trophies	Friends Only
Hidden Games	
Games	Friends Only
Requests to Watch	Friends Only
Music	Friends Only



Friends | Connections

Control who can be and see your Friends, Followers, and other connections.

Friends	Friends Only
Friend Requests	Anyone
Players Who Can Follow You	Friends Only
List of Your Followers	Friends Only
List of Players You Follow	Friends Only
Team Invitations	Friends Only
Players You May Know	Close Friends of Close Friends

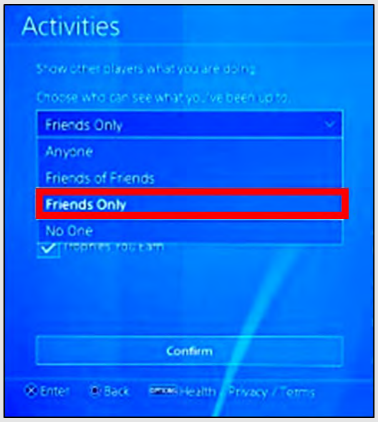


Personal Info | Messaging

Choose who can see your real name and communicate with you.

Real Name in Search	Anyone
Real Name in Friends List	Close Friends of Close Friends
Real Name in Games	Close Friends
Mobile Availability	Available
Messages	Anyone
Tags	Friends of Friends

After going through "Gaming | Media", the "Activities" box shows different setting options you can choose from for privacy. We recommend that you select the "Friends Only" option as shown here in the example picture on the right, highlighted in red.



Activities

Show other players what you are doing

Choose who can see what you've been up to.

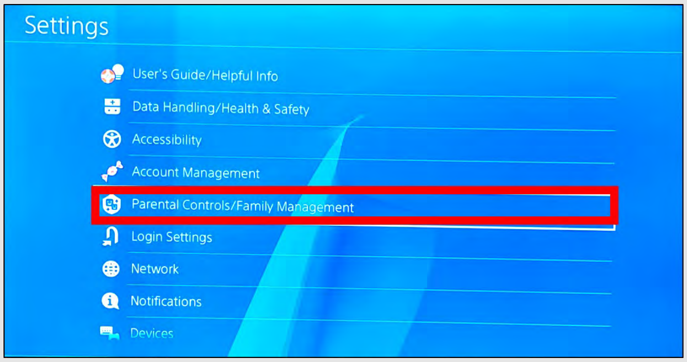
Friends Only

- Anyone
- Friends of Friends
- Friends Only
- No One

☑ Trophies You Earn

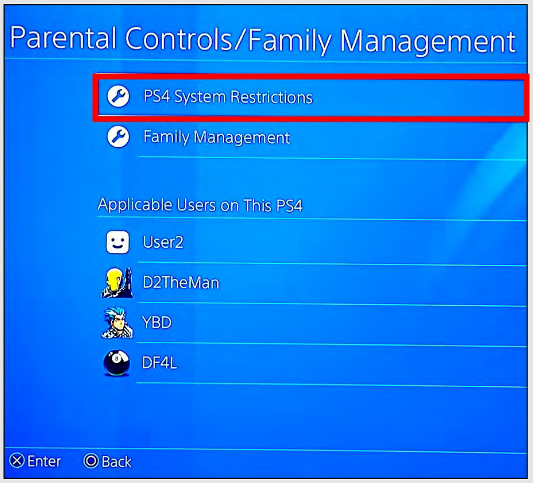
Parental Controls

PlayStation allows you to manage numerous parental control settings with the ability to limit playing time, restrict user account creation, set maturity levels for games, and change systems passcodes. To get to "Parental Controls/Family Management" settings, select the "Settings" tab on the front "Dashboard Menu" and scroll down to "Parental Controls". The subcategories are "PS4 System Restrictions" and "Family Management".



Settings

- User's Guide/Helpful Info
- Data Handling/Health & Safety
- Accessibility
- Account Management
- Parental Controls/Family Management
- Login Settings
- Network
- Notifications
- Devices



Parental Controls/Family Management

- PS4 System Restrictions
- Family Management

Applicable Users on This PS4

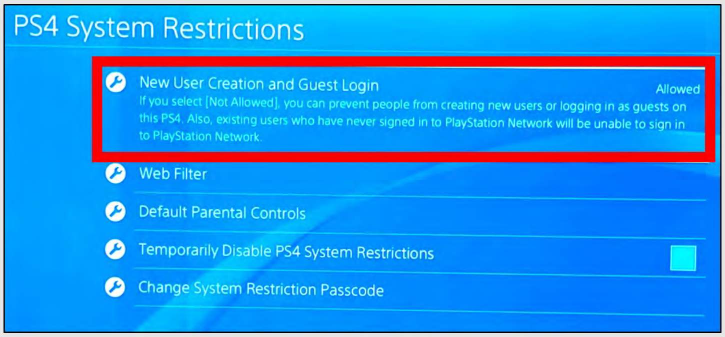
- User2
- D2TheMan
- YBD
- DF4L

PlayStation provides a login feature that utilizes facial recognition technology. The photos and derived data are stored on the system but are not shared with third parties.

UPDATED JAN 2021

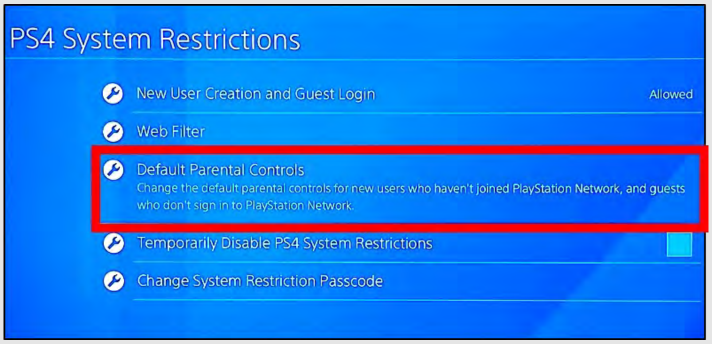
PLAYSTATION SMART CARD

From the “PS4 System Restrictions” section, you can select “New User Creation and Guest Login” to restrict who can log into the PlayStation and whether guests can access the system. From the “PS4 System Restrictions” section, you can click “Default Parental Controls” for the purpose of setting age and maturity restrictions for your users. See the graphics below highlighted in red for the pathways of these features within the settings. Parents are recommended to implement the various system restrictions and the age appropriate parental controls.



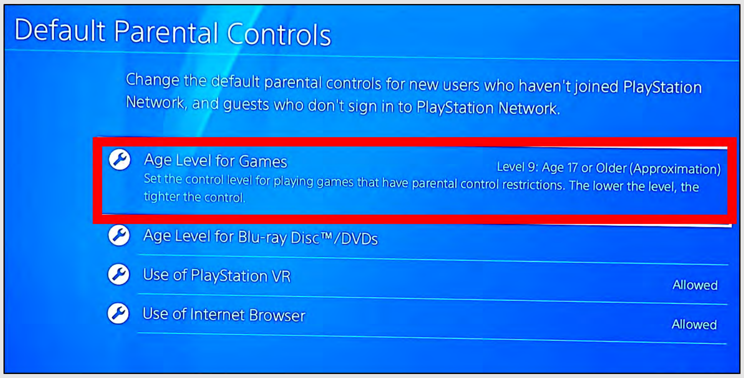
PS4 System Restrictions

- New User Creation and Guest Login — Allowed
  If you select [Not Allowed], you can prevent people from creating new users or logging in as guests on this PS4. Also, existing users who have never signed in to PlayStation Network will be unable to sign in to PlayStation Network.
- Web Filter
- Default Parental Controls
- Temporarily Disable PS4 System Restrictions
- Change System Restriction Passcode



PS4 System Restrictions

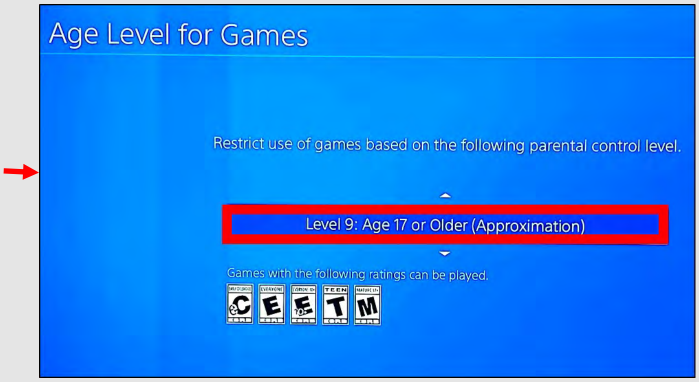
- New User Creation and Guest Login — Allowed
- Web Filter
- Default Parental Controls
  Change the default parental controls for new users who haven't joined PlayStation Network, and guests who don't sign in to PlayStation Network.
- Temporarily Disable PS4 System Restrictions
- Change System Restriction Passcode



Default Parental Controls

Change the default parental controls for new users who haven't joined PlayStation Network, and guests who don't sign in to PlayStation Network.

- Age Level for Games — Level 9: Age 17 or Older (Approximation)
  Set the control level for playing games that have parental control restrictions. The lower the level, the tighter the control.
- Age Level for Blu-ray Disc™/DVDs
- Use of PlayStation VR — Allowed
- Use of Internet Browser — Allowed



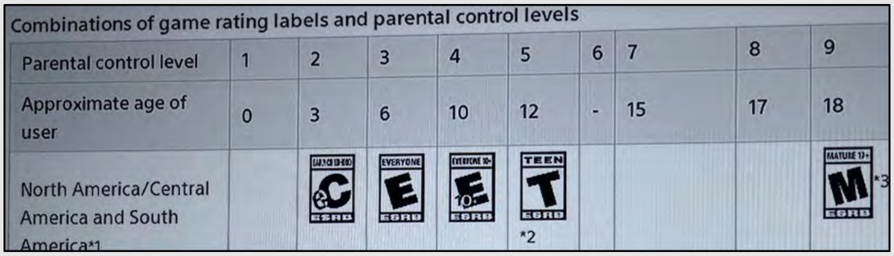
Age Level for Games

Restrict use of games based on the following parental control level.

Level 9: Age 17 or Older (Approximation)

Games with the following ratings can be played.

See below for the approximate user ages that match up to the parental control levels available in the user settings.

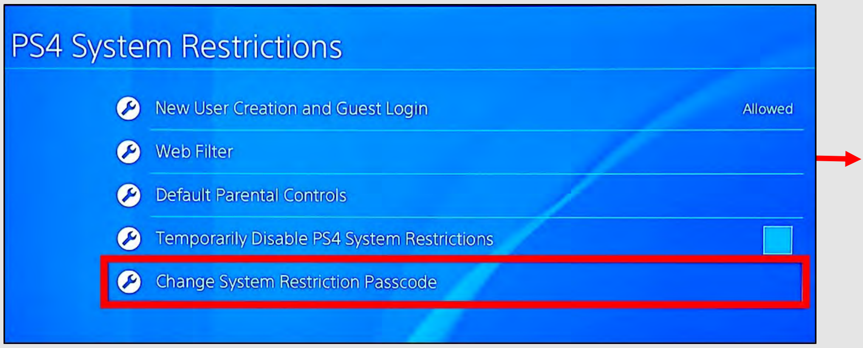


Combinations of game rating labels and parental control levels

Parental control level	1	2	3	4	5	6	7	8	9
Approximate age of user	0	3	6	10	12	-	15	17	18
North America/Central America and South America*1		EARLY CHILDHOOD eC ESRB	EVERYONE E ESRB	EVERYONE 10+ E 10+ ESRB	TEEN T ESRB *2				MATURE 17+ M ESRB *3

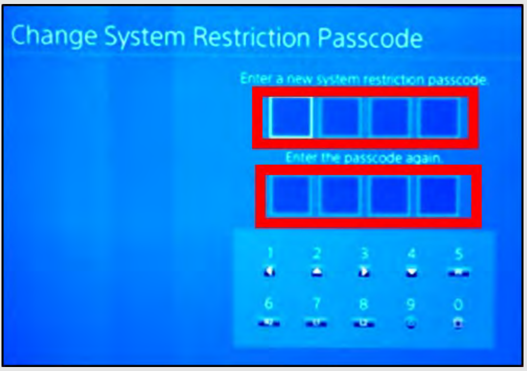
Passcode

The PlayStation Passcode is defaulted to “0000”. We recommend you change the system passcode to enhance the security of your device. To change the passcode, go to the “PS4 System Restrictions” section, and select “Change System Restriction Passcode” as illustrated in the bottom left graphic below, highlighted in red. Next, type in a new system restriction passcode. Verify the passcode by entering it twice.



PS4 System Restrictions

- New User Creation and Guest Login — Allowed
- Web Filter
- Default Parental Controls
- Temporarily Disable PS4 System Restrictions
- Change System Restriction Passcode



Change System Restriction Passcode

Enter a new system restriction passcode.

Enter the passcode again.

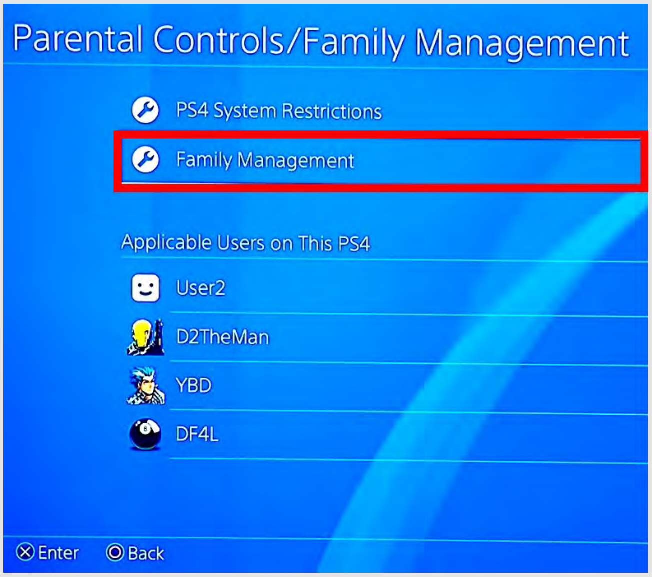
Parental controls are a means to protect children from online predators and prevent children from accessing content that is not appropriate for their age levels.

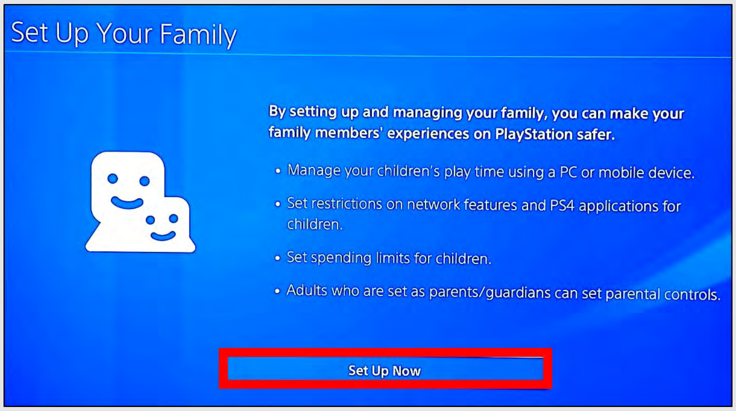
UPDATED JAN 2021

PLAYSTATION SMART CARD

Family Management

Go to the “Parental Controls/Family Management” section. On the PS4, select “Family Management” (as seen on the right, highlighted in red) and click “Set Up Now” (as seen below, highlighted in red). Within the “Family Management” area, parents can identify all the family members that will use the PlayStation system, manage play time limits, and set restrictions for children. A parent, guardian, or family manager can set the parental controls.



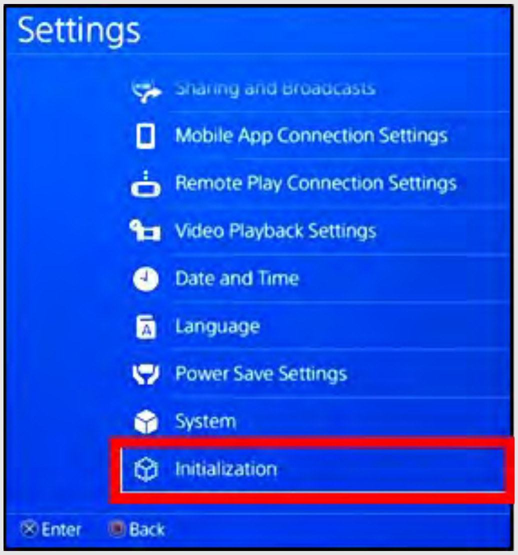


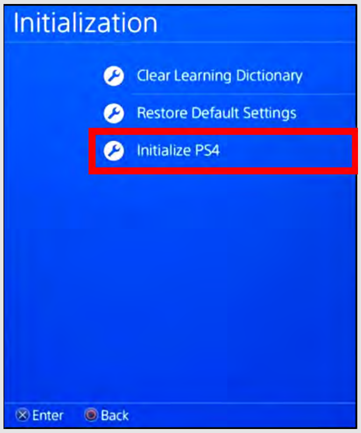
By setting up and managing your family, you can make your family members' experiences on PlayStation safer.

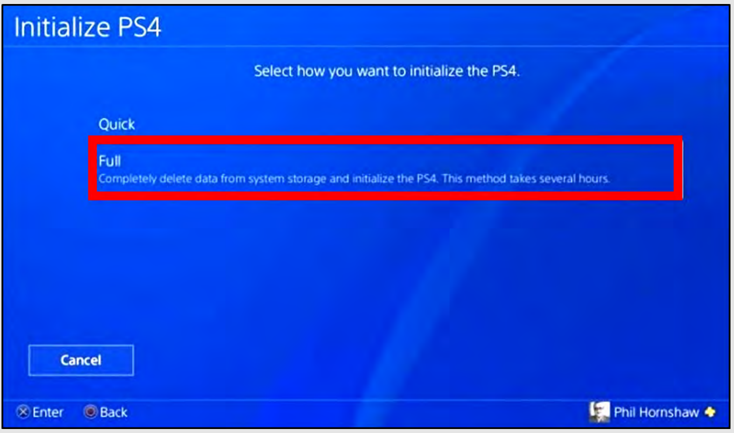
- Manage your children's play time using a PC or mobile device.
- Set restrictions on network features and PS4 applications for children.
- Set spending limits for children.
- Adults who are set as parents/guardians can set parental controls.

Initialization

Next, we recommend you use the “Initialization” feature whenever you are discarding or transferring the PlayStation system to another person. Initialization of your PS4 system restores system settings to default values. It deletes data saved on system storage and deletes all users and their data from the system. When you initialize the system software, all settings and information saved on your PS4 system are deleted. This cannot be undone, so make sure you do not delete any important data by mistake. Deleted data cannot be restored. Initialization helps ensure the removal of your privacy information after you are done with the system. In order to “Initialize” the PS4, first go to “Settings”, then “Initialization” as seen to the right, highlighted in red. Next, select “Initialize PS4” as illustrated on the bottom left, highlighted in red. Finally, click “Full”, as depicted on the bottom right graphic, highlighted in red. Selecting “Full” completely initializes the system. If the “Quick” feature is selected, the system will not be completely restored to a default system - some data will still remain on the PS4. Be sure you are doing a “Full” initialization.







Select how you want to initialize the PS4.

Completely delete data from system storage and initialize the PS4. This method takes several hours.

Users should never discard systems or devices that still have personal information retained on the device. When possible, always return the device back to factory settings.

UPDATED JAN 2021

PLAYSTATION SMART CARD

Potential System Compromise:

Do you think your account may have been compromised or hacked? Have you noticed any of the following:

- Unexpected charges from financial institutions tied to your PlayStation accounts.
- Primary email and password have been changed without your authorization.
- Other account behaviors you didn't perform or approve (like following, unfollowing, blocking, etc.).
- Primary console changed to another device without your consent.
- Receive a special character in a private message, immediately followed by the system crashing or frequent glitches.

If you said “Yes” to any of the above, you are recommended to take the following actions:

- Change your password immediately and use strong/complex passwords.
- Enable two-factor verification.
- Notify the financial institutions about fraudulent purchases resulting from the hack.
- Set your “Messages” privacy setting to “Private” and adjust other privacy settings as well.
- Restrict who has access to create new accounts and logins.
- Contact PlayStation Support or the Sony Customer Service line immediately.

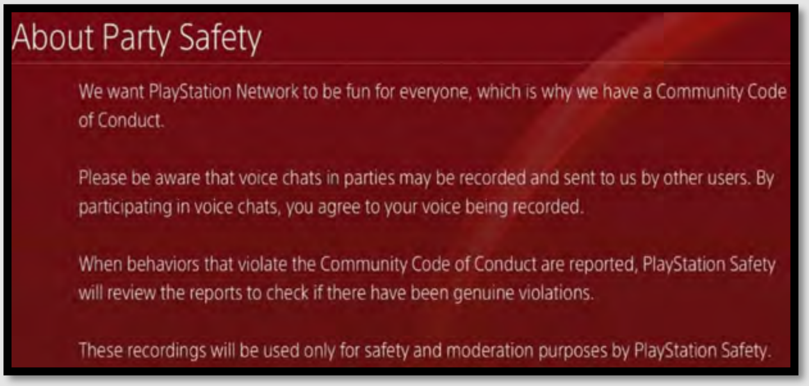
If you need to report **Spam/Fake Accounts/Harassment**: Contact the PlayStation Support Site at 1-800-345-7669 or the Sony Customer Service Line.

Also, you can report that your account has been hacked by going to https://support.playstation.com.

If you have additional questions about responding to system compromise, contact https://twitter.com/AskPlayStation/.

Important Message on PlayStation: you are responsible for all activities on your PlayStation Network, so it’s very important you do your best to ensure you are the only person using it.

The PlayStation System is an entertainment system that enables users to enjoy multiplayer online gaming, stream live TV, provides a social and messaging network for friends to connect, allows for video streaming services such as Netflix, Amazon Video, Hulu, YouTube, HBO Now, NBA TV, and more. Each application has its own privacy concerns and is susceptible to being breached or hacked.



About Party Safety

We want PlayStation Network to be fun for everyone, which is why we have a Community Code of Conduct.

Please be aware that voice chats in parties may be recorded and sent to us by other users. By participating in voice chats, you agree to your voice being recorded.

When behaviors that violate the Community Code of Conduct are reported, PlayStation Safety will review the reports to check if there have been genuine violations.

These recordings will be used only for safety and moderation purposes by PlayStation Safety.

Sony/PlayStation Users recently received a notification like the one on the left here. This notification is to let users know that there has been a change in their policy and they are not allowing users to record party conversations. This does not mean however, according to Sony, that Sony or PlayStation themselves are recording your conversation. These recording must be initiated by an individual in the “Party” and then submitted for possible violations to Sony. This feature is also only available to PS5 users but can be used in parties where PS4 users are also in attendance.

UPDATED JAN 2021

Hidden Phone Apps

What are Hidden Apps?

"Hidden" apps, "Vault" apps and "Ghost" apps, are apps that look innocuous, perhaps like a calculator, but are actually used to hide pictures, videos and messages on a smart device. Teens often use these apps because they want to hide their activity from their parents. Most times, these apps require a password to be entered in order to gain entry into the hidden area of the app. Some Vault apps go a step further and if the password is entered incorrectly, a picture of the individual attempting to gain access will be taken.

Android Hidden Apps (some examples)	
	1 Gallery Vault - hide pictures & videos, strong encryption
	LockMyPix - hide photos, videos, AES encryption
	Vaulty - hide pictures and videos
	Keepsafe Photo Vault - hide private photos and videos
	Vault - Hide pics and video

iPhone Hidden Apps (some examples)	
	Fake Calculator App - hide photos and videos (many versions)
	Private Photo Vault - picture safe
	Secret Calculator Fake Vault
	Keepsafe Photo Vault - hide private photos and videos
	Secret Vault Hide Photos - private picture safe

Do's and Don'ts

- ***Do*** periodically check your child's smart devices to make sure they have not downloaded anything you have not approved.
- ***Do*** think about using a monitoring service (as discussed in the Keeping Children Safe Online Smart card) for your child/teens smart devices, especially if you have given them the ability to download apps themselves.
- ***Do*** talk to your teens about the dangers of taking and sending nude photos or videos on their smart devices and make sure they understand the serious consequences.
- Do ***not*** give your child/teen the password or authorization to download apps in their respective "App Store". Having them ask you for the password allows you to review any app they might want to put on their device.
- Do ***not*** allow your child to use "Messaging Apps" that instantly delete the content they hold. Allowing such apps will take away from your ability to help your kids navigate through smart device social norms.
- Do ***not*** allow children to set private passwords without sharing them with you. Always ensure that you can access your child/teen's phone at any time.

According to MediaSmarts research twenty-six per cent of students in eighth grade said a sext they sent was forwarded to other people by the recipient. #protectourchildren

UPDATED JAN 2021

Hidden Phone Apps

How to find “Hidden Apps”

- One of the easiest ways to search for hidden apps on a smart device is to visit the devices respective App store (Apple or Google Play Store).
  - **Android device-** In the “Google Play Store” select “Menu” (3 vertical lines in the “Search” box), then select “My apps & games.” Next, select the “Installed” tab in the middle of your screen. Here you can review all the apps that have been downloaded to the device. Additionally, from your “Account” (under the same “Menu”) you can review “Purchase History” which will provide you an overview of all purchased apps.
  - **iPhone device-** In the “App Store” find and select the “Account” icon, or “Profile Picture” at the top right of your screen. Then select “Purchased” and the account you want to review purchases from (if you have an “Apple Family Sharing Plan”, more than one account will appear).
- Another way to review purchase history on a smart device is to find the “App Store” and search for “Hidden Apps.” Once a list of available apps appears on the screen, you can scroll through the list. If any “Hidden Apps” are downloaded on the device, it will be noted to the left side of the screen. This method may return inaccurate results due to some apps being miscategorized.

You can limit the amount of time your child spends on his/her device unsupervised, by ensuring he/she puts it in the kitchen or living room before bed.

Red Flag Indicators

I. If your child seems to have more than one of any kind of app it may indicate that one of those apps is not what it appears to be. Redundancy in apps may indicate that one is a “Hidden App”.

II. If your child seems to try and hide his / her screen any time you enter the room, it may indicate he / she is trying to hide his / her phone activity from you.

How to Prevent Your Child from Downloading Hidden Apps

- **On iPhone**: iOS has an “Apple Family Sharing Plan” that allows parents to turn on a feature called “Ask to Buy”. When this feature is enabled, your child will not be able to download any apps without your approval.
- **On iPhone**: iOS has a built in feature that can be controlled through the “Settings” of your iPhone. Simply go in to your “Settings” section and find “Screen Time”. Select “Turn On Screen Time” > “Continue” > “This is My Child’s iPhone” > “Not Now” > “Not Now”. From there you can go in and set “Content & Privacy Restrictions” as well as a “Use Screen Time Passcode” to make sure that your settings are not changed by anyone who doesn’t have a password.
- **On Android**: Android users can setup parental controls in the “Google Play Store” by creating a PIN and choosing the maturity levels you want to allow. Go to the “Google Play Store” > “Menu” > “Settings” > under “User Controls”, you will find “Parental Controls”, and other settings you can review to control what your children download. It is also important to note that where many of the “Hidden Apps” are concerned, “Google Play Store” rates them “E” for everyone.
- **On Android**: Android users can also create a password for authentication to authorize purchases. This feature is located in the “User Control” section of your “Google Play Store” “Settings”.

UPDATED JAN 2021

Pay Apps

G Pay

Pay

Do's and Don'ts

- ***Do*** review all privacy settings, and set them in accordance with your personal preference and acceptable risk level. Some mobile pay apps have a social side to them which may display your payment activity if not locked down.
- ***Do*** make sure you have an anti-malware app on your phone to protect your phone, and the information on your phone from getting into the wrong hands.
- ***Do*** make sure to periodically check transactions made on mobile pay apps. Make sure they are accurately showing up on the payment device you have linked to the app.
- Do ***not*** visit online banking or online shopping websites by clicking on a link you have received in an email or from a text message. Doing so may lead to fictitious websites and possible identity theft.
- Do ***not*** use unsecured Wi-Fi or public Wi-Fi networks while using mobile pay apps or for any online banking purposes.
- Do ***not*** download mobile pay apps from unofficial sites. It is recommended for all apps, not just mobile pay apps, that you use official stores such as the Apple and Google Pay stores.

DEFINITION

Mobile wallets utilize technology you already own— your smartphone, for example — to allow you to make in-store payments quickly and securely without having to use your credit or debit card. The term "digital wallet" may refer to either an electronic device that stores payment information (such as a smartphone) and the program or app used to make the payment, such as Apple Pay, Google Wallet, Samsung Pay, or PayPal.

Risks

Using mobile pay apps means that losing your phone essentially becomes that equivalent of losing your wallet. Whoever finds your phone holds the keys to your identity.

Using pay apps via your smart device means having to be on the alert for cyber criminals.

Using mobile pay apps means you may run the risk of malware infecting your phone and gaining access to payment and identity information.

Gains

Unlike your wallet, if your cell phone is stolen or even misplaced, there are levels of security that will limit or even prevent anyone from accessing the contents of your smartphone. Additionally, the user usually has the ability to "wipe" (delete all personal information) their phone if they feel it has been compromised or simply cannot be found, unlike a physical wallet which becomes immediately compromised.

Using physical debit or credit cards means you run the risk of having your card copied upon scanning it if the machine being used has been tampered with.

The privacy policy for each "Pay App" states what agreements a user consents to when signing up for the application. While each app has different information that is stored and/or shared, they all have a common theme. Many applications collect your name, date of birth, email address, telephone number, name of financial institution, financial account numbers, additional information from consumer reporting agencies, people you invite to use the application, the operating system on the device, etc. The company may be able to keep your information for an indefinite period of time, depending on what the privacy policy states.

Even if you rely solely on mobile pay apps to make your purchases, it is important to have some other form of payment handy in case you are unable to access your phone.

UPDATED JAN 2021

Pay Apps

App	Apple Pay	Venmo	Facebook Messenger	Cash	Zelle	Xoom	Google Pay
Security	High	Low-Medium	Medium-High	Medium-High	High	Medium-High	High
International Pay Feature	Yes, User must manually turn this feature on	No	Yes, limited	Yes, UK	No	Yes	Yes
Linked to Bank Account	Transfer to Bank account	Yes	Yes, only through a Visa or Mastercard debit card or Paypal account	Yes	Yes	Yes	Yes
Linked to Debit Card	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Linked to Credit Card	Yes + Fee	Yes +Fee	Yes	Yes + Fee	No	Yes	Yes
Paying on the Web	Yes if accepted and while using an Apple device.	Yes, if accepted and while using a smart device where App is loaded.	Yes, thru Facebook ads, Marketplace and groups. **See Cons	Yes, with Cash Card or other payment system such as Google Pay	No	Through Paypal	Yes if accepted
In Store Payments	Yes, where accepted	Limited acceptance at retailers.	No	Yes, with Cash Card or other payment system such as	No	No	Yes

	Apple Pay	Venmo	Facebook Messenger	Cash	Zelle	Xoom	Google Pay
Pros	Rated most secured payment app. Accepted at some major universities	User friendly. owned by PayPal	Secure payment method for friends and family. User friendly.	Easy to use and friends do not need the app to receive money. Can purchase and sell Bitcoin.	Works directly with your bank app.	Offers a money back guarantee, pay bills and reload mobile phones. Powered by PayPal.	Widely accepted, easy to use. Able to use on Android and IPhone devices.
Cons	Transfers can only be made to other Apple device users. Only works with Apple devices.	**Default privacy setting shares your payment history with the world.** Scammers are known to take advantage of Venmo.	Limited use. No ability to stop a payment on your end once you send it (however, receiver can reject it). Payment protection only applies to payments made to family and friends.	Not widely accepted. Customer service limited to messaging in app, no call center.	If money is sent to the wrong person or user becomes a victim of fraud or scam, Zelle will not reimburse you.	There is a minimum payment for use. Requires Gov. issued ID as well as a proof of residents. They may also require a bank statement.	In order to use Pay to Pay (pay a friend etc.) you have to download the Google Pay Send App separately.

Use any available password protection for your smart device - two-factor authentication, phone log on password - to ensure the protection of your data.

UPDATED JAN 2021

DATING SITE BEST PRACTICES

#DATESAFE

Do’s and Don’ts

- ***Do*** protect your information and set limits on what and when you provide information to people you meet on dating sites.
- ***Do*** provide your own transportation when meeting an individual for the first few times
- ***Do*** use more popular dating apps and stay away from less popular sites, which may have less security in place.
- Do ***not*** use dating app sites on any public Wi-Fi. It is important to always make sure you are connected through a secure internet connection.
- Do ***not*** synch your social media accounts with your dating accounts.
- Do ***not*** forget to trust your “gut”. If something doesn’t feel or seem right it very likely isn’t.
- Do ***not*** give out personal information right away to include personal numbers or email addresses.

- **Be Anonymous - Don't include your last name or any other identifying information in your profile or initial communications. Likewise, we recommend you *not* include your contact information - email address, home address, phone number - on your profile**
- **Create a unique email address and Username for Dating Apps**
- **Keep your financial information private!**
- **Do *not* meet at your house or place of work**
- **Do *not* ask or allow a lot of personal questions initially. Save that for the date, this will help to prevent you from giving away too much information, too early.**
- **Do avoid drinking too much during your first several dates. Wait to loosen up until you get to know your date a little better.**
- **Try to do a search of your date on the internet before meeting up (see Self Assessment Smart-Card).**
- **Online dating scams are known to run as long as six months before you notice anything suspicious. Always be on the lookout for unusual conversations and behavior, such as your date requesting money or suddenly needing a ride somewhere.**

Things to watch out for:

- An early request for photographs or videos
- A request for money or donations
- Minors using the platform!
- Users sending harassing or offensive messages
- Users behaving inappropriately after meeting in person
- Fraudulent profiles - if a profile looks incomplete or too good to be true, it probably is.

If someone immediately directs you to a different website from the one you are already on, you could be dealing with a scammer. #themoreyouknow

UPDATED JAN 2021

DATING SITE BEST PRACTICES

When you decide to give someone your phone number, use your cell rather than your home or work phone. If things don't work out, cell phone numbers are easier to change.

HOOKUP APPS: Tinder, Happn, HUD, Bumble, Hinge

A hookup app is one that accepts and encourages casual sexual encounters or "hookups", including one-night stands and other related activity, without promising or requiring emotional bonding or long-term commitments. These types of sites pose serious dangers to their members because they usually involve meeting up with strangers. A lot of trust is expected in such a situation, where no justification is provided.

If you choose to use a "hookup app", it is important to let someone you trust know where you are going and with whom, whenever you decide to "meet up" with someone you don't know well. These apps may not be intended to be used only for "hooking up" and can also be used to develop meaningful relationships. In reality however, that is not their primary function.

CASUAL DATING SITES: Match, Zoosk, Plenty of Fish, OkCupid, EliteSingles

Online dating services such as these allow users to become "members" by creating a profile and uploading personal information including (but not limited to) age, gender, sexual orientation, location, likes and dislikes. Most of these services offer digital messaging, as well as online chat, telephone chat (VOIP), and message boards. Members can constrain their interactions to the online space, or they can arrange a date to meet in person. These dating sites usually attract people looking for something a bit more long term than a "hookup", and have more chance of leading to a relationship. In fact many of these sites allow you to declare your dating and commitment intentions.

These sites target specific demographics based on features like shared interests, location, religion, or relationship type. Most are completely free and depend on advertising for revenue. Others offer a free registration and use, with optional paid premium services.

Larger Dating Apps: eHarmony, Christian Mingle, Farmers Only

Online dating services such as these tend to be more methodical in their matching of partners. They usually have a signature questionnaire that helps to match people based on compatibility of shared interests, and further, in terms of emotional and relationship values. These sites offer more nuanced compatibility ratings than the "hookup" and "casual dating" apps, and are targeted towards clients looking for longer term relationships.

These apps offer more services than the others. For instance, the app may guide you through the initial stages of your relationship by helping you to pace communication with your matches so that each of you remains comfortable, and things don't move too quickly.

These sites usually require a form of payment and a membership for access to full content. Generally, these are sites people use when they are seeking a deeper connection and long term relationship or marriage.

"Millions of Americans use dating sites, social networking sites, and chat rooms to meet people. And many forge successful relationships. But scammers also use these sites to meet potential victims. They create fake profiles to build online relationships, and eventually convince people to send money in the name of love. Some even make wedding plans before disappearing with the money.

An online love interest who asks for money is almost certainly a scam artist."

-Federal Trade Commission

UPDATED JAN 2021

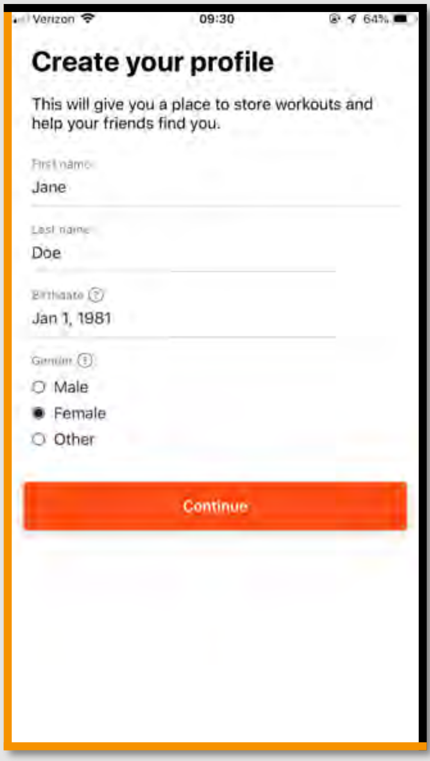
Fitness Apps

Mobile Device Version

*** This information describes how to make your account secure on Android and iPhone mobile devices. Differences between iPhone Operating System (iOS) and Android Operating System (AOS) are minimal, in such cases iPhone images are outlined **orange** and Android **black**.*

Do's and Don'ts

- ***Do*** make sure that your profile is not set to "public". Also, limit what information you put on your profile even if it is set to "private".
- ***Do*** keep your fitness app *activity* set to "private" by default, so that your routes cannot be tracked online.
- ***Do*** ensure that family members take similar precautions with their accounts.
- ***Do*** use a picture of something other than yourself for your profile photo. Profile photos are viewable to the public.
- Do ***not*** link your fitness app to any of your social media accounts. Doing so allows your routes and the times you exercise to be published to your social media accounts for others to see.
- Do ***not*** track exercises that begin at your own home, work place, or school.
- Do ***not*** chose the same route every time you go for a run or walk. It is important to mix it up so that any potential stalker won't be able to track your whereabouts.



Verizon 09:30 64%

Create your profile

This will give you a place to store workouts and help your friends find you.

First name: Jane

Last name: Doe

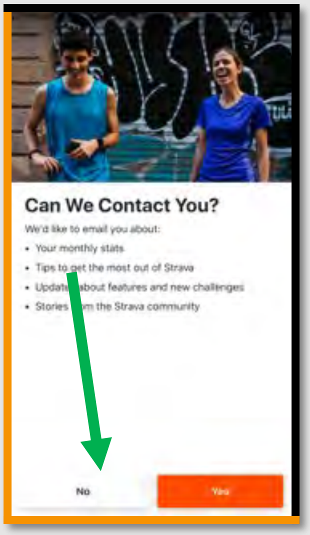
Birthdate: Jan 1, 1981

Gender
○ Male
● Female
○ Other

Strava Activity Tracker

Strava is a fitness tracker as well as a social network, its key feature is that its members can locate the most popular bike and running paths in their areas, follow their friends' routes, and log group exercises. For these key features to work, an optimal number if members must continuously be sharing location data. In other words, if you want to get the most out of Strava, you need to share your location data, but this comes with a big privacy trade-off.

Late last year Strava's heat map came under fire for posting its users' locations publicly online. If you leave your location data for people to see, you become vulnerable to victimization, for instance of physical attack, stalking, or theft of your belongings when you are away from your home. The following describes the best way to create an account on Strava, while maintaining the utmost privacy to ensure your safety.



Can We Contact You?

We'd like to email you about:

- Your monthly stats
- Tips to get the most out of Strava
- Updates about features and new challenges
- Stories from the Strava community

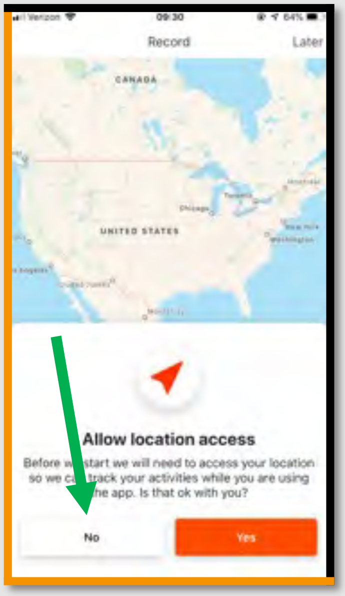
Create Your Profile

Start by creating your account, only putting in the minimum personal information required to create your log on (shown here to the left). Later you will have the option to build upon your "Profile" by adding additional information about yourself, but we recommend keeping as little personal information on your profile as you can..

Next (shown on the top right), you are asked if you would like Strava to push monthly reports to your email. We recommend you decline this option because it is possible for Strava to then share additional information with you, or about you to others. Select the "No" option.

The next screen asks if you will allow Strava to access your location. Although this is a big part of the app, we strongly recommend you ***not*** allow Strava to have access to your location.

You will also be asked several times to synch your contacts to the Strava app during set up. We recommend, anytime you are asked, that you ***not*** synch your contacts to this app.



Verizon 09:30 64%

Allow location access

Before we start we will need to access your location so we can track your activities while you are using the app. Is that ok with you?

Always go back and check the privacy settings in your fitness app after an update has taken place to ensure they remained intact.

Fitness Apps

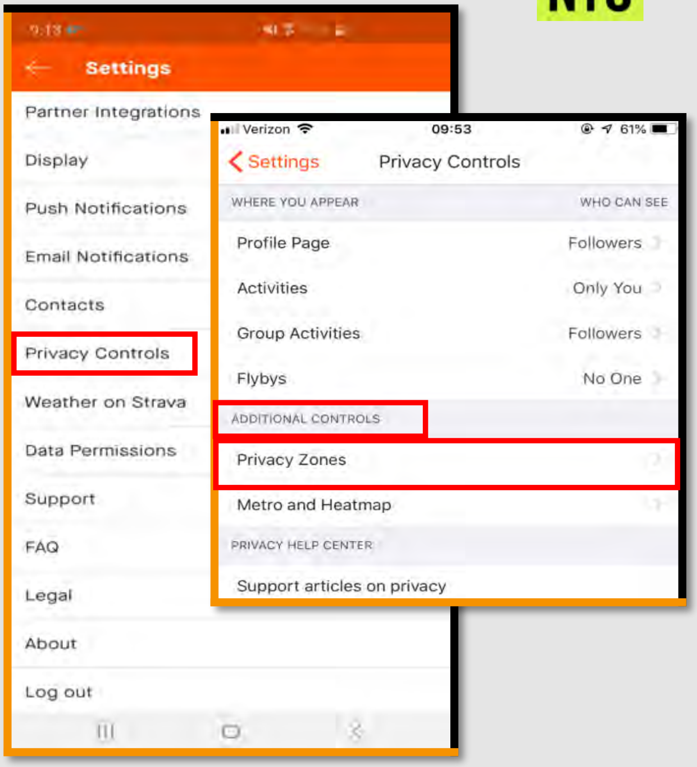
Mobile Device Version

*** This information describes how to make your account secure on Android and iPhone mobile devices. Differences between iPhone Operating System (iOS) and Android Operating System (AOS) are minimal, in such cases iPhone images are outlined orange and Android (and when both are same)* ***black****.*

Who can see your routes?

Once you have completed the set-up process, there are several settings that must be set in order to best protect your privacy. From the "Home" screen, look to the bottom of the page and select "Profile" then select the "Settings" icon (looks like a wheel) at the top right of your screen. In the "Settings" section scroll down and select "Privacy Controls" (see right). Under "Privacy Controls" it is recommended that you change all of the tabs under "Where You Appear" from "Public" to either "Followers" or "Only You" to maximize your privacy.

The "Privacy Zones" function, under "Privacy Controls" > "Additional Controls", allows you to draw a privacy circle around a certain area such as your house or work. When you run in that circle you are automatically hidden from all other users. The down side is that if you step outside of that designated circle, that data will become public automatically.



Settings

- Partner Integrations
- Display
- Push Notifications
- Email Notifications
- Contacts
- Privacy Controls
- Weather on Strava
- Data Permissions
- Support
- FAQ
- Legal
- About
- Log out

Verizon 09:53 61%

Settings Privacy Controls

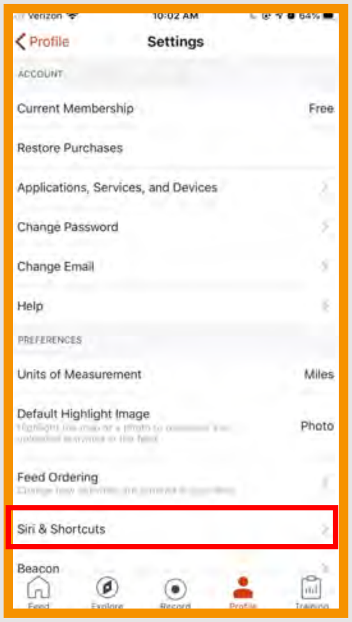
WHERE YOU APPEAR	WHO CAN SEE
Profile Page	Followers
Activities	Only You
Group Activities	Followers
Flybys	No One

ADDITIONAL CONTROLS

- Privacy Zones
- Metro and Heatmap

PRIVACY HELP CENTER

- Support articles on privacy



Verizon 10:02 AM 64%

Profile Settings

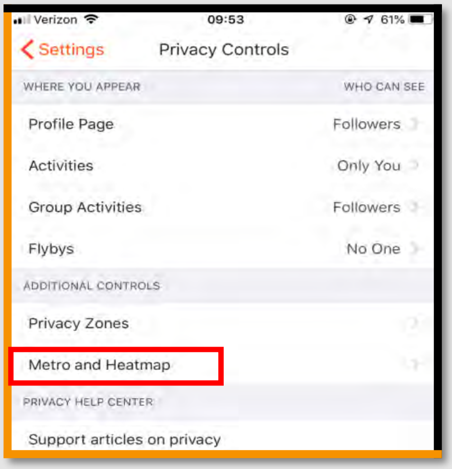
ACCOUNT

Current Membership	Free
Restore Purchases	
Applications, Services, and Devices	
Change Password	
Change Email	
Help	

PREFERENCES

Units of Measurement	Miles
Default Highlight Image	Photo
Feed Ordering	
Siri & Shortcuts	
Beacon	

On iPhone: we recommend you scroll to the "Siri & Shortcuts" tab, under "Settings" (see left) and review the current settings there. Ensure your "Siri" function is off.



Verizon 09:53 61%

Settings Privacy Controls

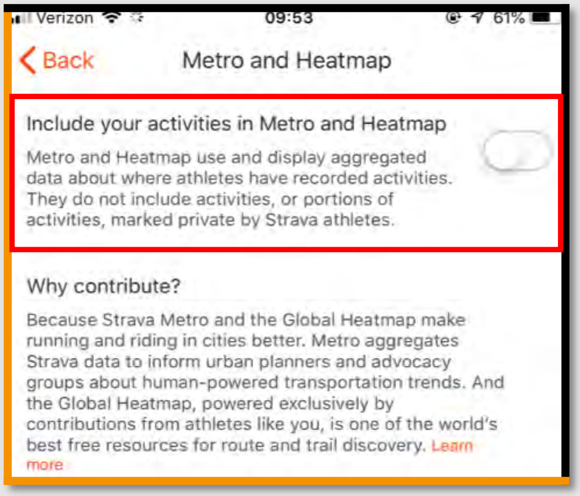
WHERE YOU APPEAR	WHO CAN SEE
Profile Page	Followers
Activities	Only You
Group Activities	Followers
Flybys	No One

ADDITIONAL CONTROLS

- Privacy Zones
- Metro and Heatmap

PRIVACY HELP CENTER

- Support articles on privacy



Verizon 09:53 61%

Back Metro and Heatmap

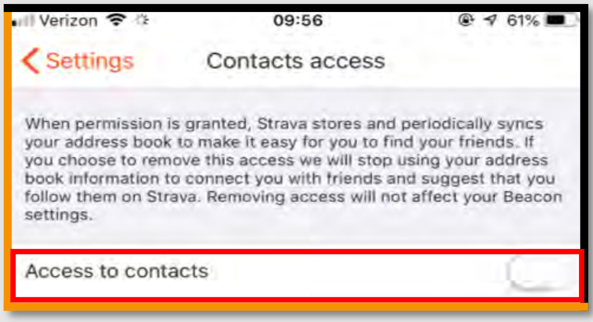
Include your activities in Metro and Heatmap

Metro and Heatmap use and display aggregated data about where athletes have recorded activities. They do not include activities, or portions of activities, marked private by Strava athletes.

Why contribute?

Because Strava Metro and the Global Heatmap make running and riding in cities better. Metro aggregates Strava data to inform urban planners and advocacy groups about human-powered transportation trends. And the Global Heatmap, powered exclusively by contributions from athletes like you, is one of the world's best free resources for route and trail discovery. Learn more

Next, we recommend you turn the "Metro and Heatmap" function off. This feature allows Strava to collect data and recordings from your device. First, under "Privacy Controls", go to "Metro and Heatmap", then next to "Include your activities in Metro and Heatmap", set the toggle to "Off", as seen above.



Verizon 09:56 61%

Settings Contacts access

When permission is granted, Strava stores and periodically syncs your address book to make it easy for you to find your friends. If you choose to remove this access we will stop using your address book information to connect you with friends and suggest that you follow them on Strava. Removing access will not affect your Beacon settings.

Access to contacts

Contacts

Finally, we recommend you turn off the function that allows Strava to have access to your "Contacts" - the default for this function is set to "On". Go back to "Settings", scroll to the middle of the menu, select "Contacts". Set the toggle to "Off".

Even with phone apps, it is important to make sure you keep a strong password to prevent anyone from accessing your account.

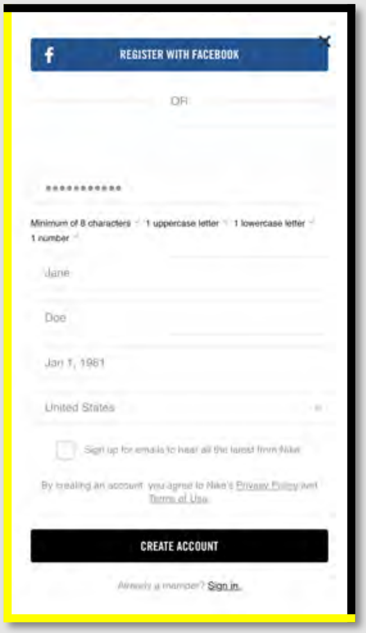
UPDATED JAN 2021

Fitness Apps

Mobile Device Version

*** This information describes how to make your account secure on Android and iPhone mobile devices. Differences between iPhone Operating System (iOS) and Android Operating System (AOS) are minimal, in such cases iPhone images are outlined **yellow** and Android **black**.*

Nike Run Club



REGISTER WITH FACEBOOK

OR

••••••••••••

Minimum of 8 characters ✓ 1 uppercase letter ✓ 1 lowercase letter ✓ 1 number ✓

Jane

Doe

Jan 1, 1981

United States

□ Sign up for emails to hear all the latest from Nike

By creating an account, you agree to Nike's Privacy Policy and Terms of Use.

CREATE ACCOUNT

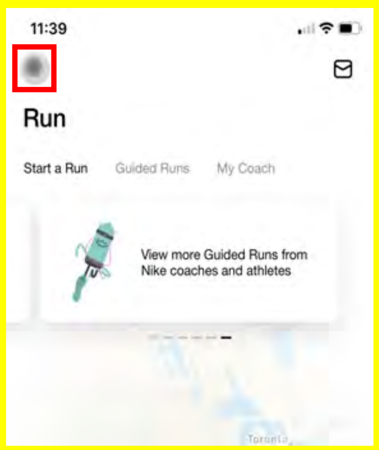
Already a member? Sign in.

The "Nike Run Club" App is one of the most popular activity tracking apps available. One of the things it does is publish your completed runs and fitness activities and stats directly to your social media accounts when you finish - this includes your running routes, which creates vulnerabilities. We recommend that as you create your Nike Run Club account, you provide the minimum amount of personal information possible. First, you will enter your "Basic Information". Remember, never allow one app to have access to another - so do not log in via Facebook or another social media account. Instead, use an email and password unique to this account. Also, we recommend you ***not*** allow this app to access your location.

Who can see my info?

First, let's go to the "Settings" and establish your "Privacy" settings.

On Android: select the "Menu" option at the top left of the screen, then select "Settings" at the bottom of the list. (see right)

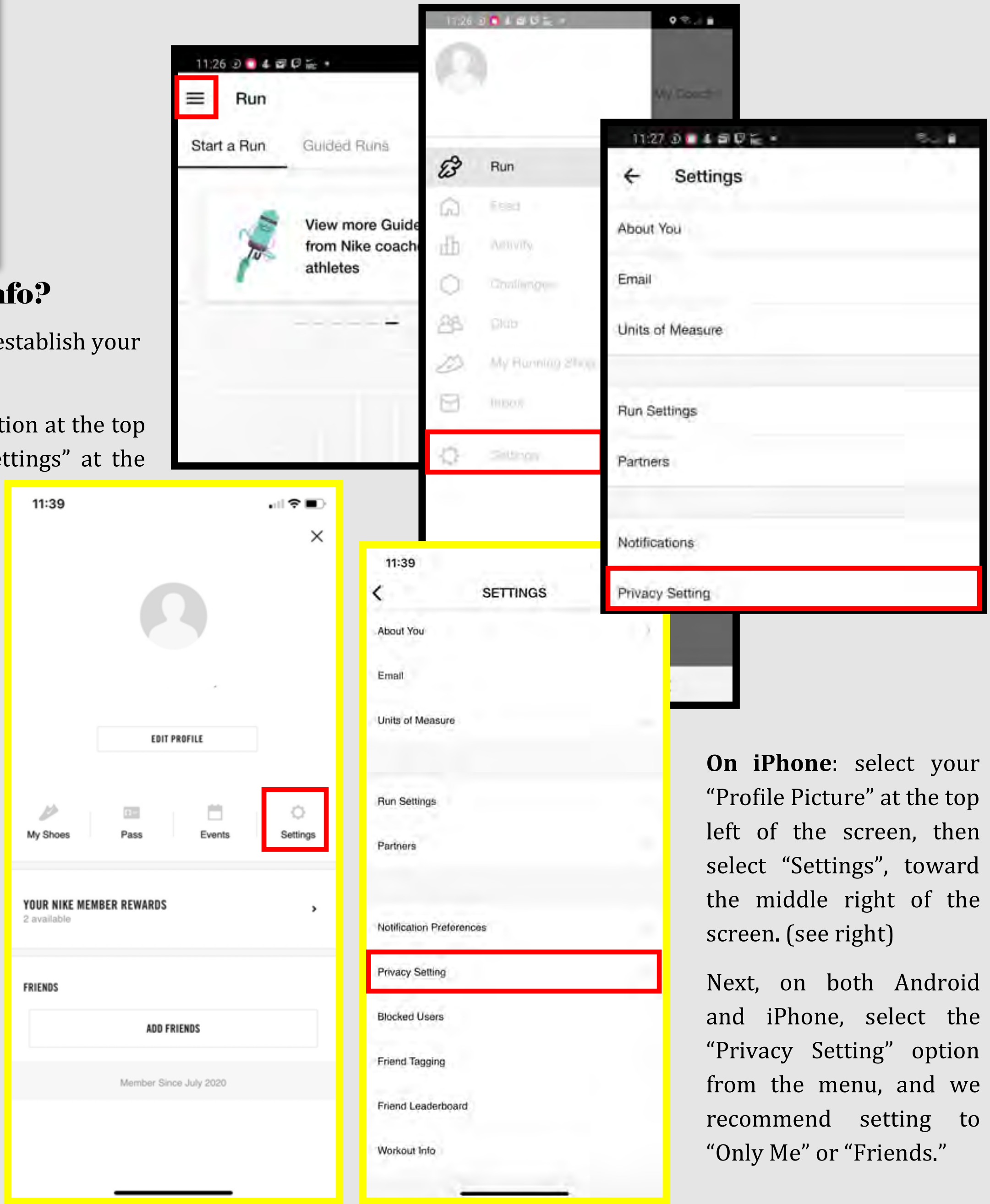


11:39

Run

Start a Run · Guided Runs · My Coach

View more Guided Runs from Nike coaches and athletes



11:26

Run

Start a Run · Guided Runs

View more Guided Runs from Nike coaches and athletes

Run · Feed · Activity · Challenges · Club · My Running Shop · Inbox · Settings

11:27

Settings

About You

Email

Units of Measure

Run Settings

Partners

Notifications

Privacy Setting

11:39

EDIT PROFILE

My Shoes · Pass · Events · Settings

YOUR NIKE MEMBER REWARDS
2 available

FRIENDS

ADD FRIENDS

Member Since July 2020

11:39

SETTINGS

About You

Email

Units of Measure

Run Settings

Partners

Notification Preferences

Privacy Setting

Blocked Users

Friend Tagging

Friend Leaderboard

Workout Info

On iPhone: select your "Profile Picture" at the top left of the screen, then select "Settings", toward the middle right of the screen. (see right)

Next, on both Android and iPhone, select the "Privacy Setting" option from the menu, and we recommend setting to "Only Me" or "Friends."

If you allow other third party apps to connect to your fitness app be sure to check both apps for up-to-date privacy settings.

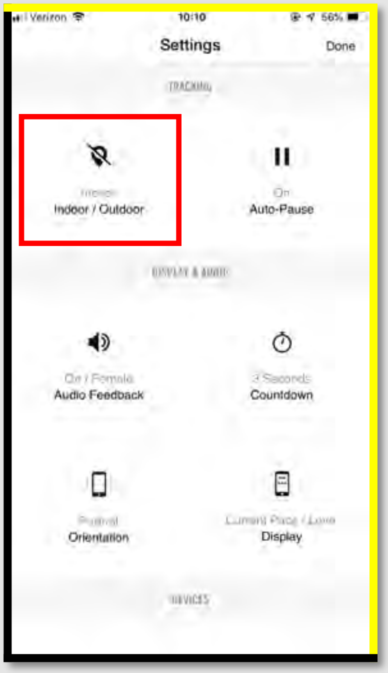
Fitness Apps

Mobile Device Version

*** This information describes how to make your account secure on Android and iPhone mobile devices. Differences between iPhone Operating System (iOS) and Android Operating System (AOS) are minimal, in such cases iPhone images are outlined* ***yellow*** *and Android* ***black****.*

Nike Run Club

Next, go back to "Settings" and visit "Run Settings". We recommend you set the "Tracking" function to "Indoor" so that the app cannot track your outdoor routes.



Verizon 10:10 56%

Settings Done

TRACKING

Indoor
Indoor / Outdoor

On
Auto-Pause

DISPLAY & AUDIO

On / Female
Audio Feedback

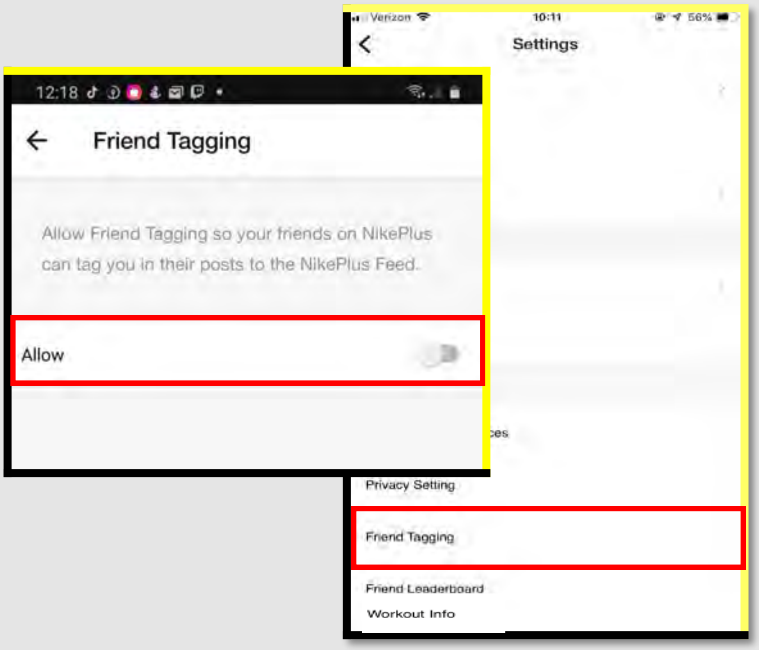
3 Seconds
Countdown

Portrait
Orientation

Current Pace / Lone
Display

DEVICES

We recommend you ***not*** allow "Friends" to "Tag" you in their posts, this is one way you really lose control over your information. Go to "Settings", then "Friend Tagging", then next to "Allow", set the toggle to "Off".



Verizon 10:11 56%

Settings

Privacy Setting

Friend Tagging

Friend Leaderboard

Workout Info

12:18

Friend Tagging

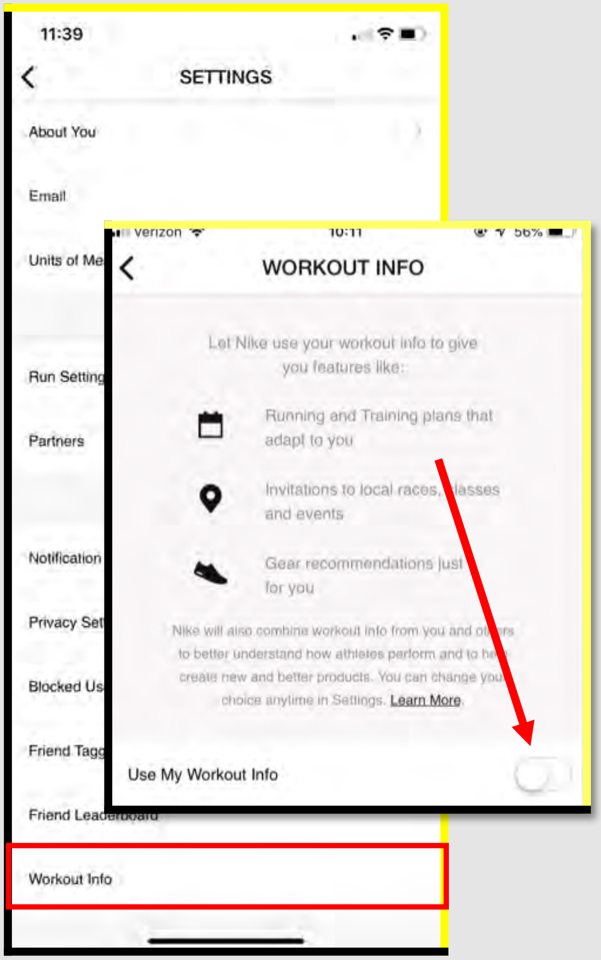
Allow Friend Tagging so your friends on NikePlus can tag you in their posts to the NikePlus Feed.

Allow

What personal data does Nike Run Club collect? Nike Run Club collects the following data in order to provide you with its products and services - unless you lock down your account:

- Contact details including name, email, telephone number, address
- Login and account information
- Personal details like gender, hometown, birthday
- Credit card information
- Images, photos, videos

Finally, let's visit the "Workout Info" function, below "Privacy Settings", which also must access your location and other personal data in order to work optimally. We recommend you set the toggle to "Off" in order to secure your data and personal information.



11:39

SETTINGS

About You

Email

Units of Me

Run Setting

Partners

Notification

Privacy Set

Blocked Us

Friend Tagg

Friend Leaderboard

Workout Info

Verizon 10:11 56%

WORKOUT INFO

Let Nike use your workout info to give you features like:

Running and Training plans that adapt to you

Invitations to local races, classes and events

Gear recommendations just for you

Nike will also combine workout info from you and others to better understand how athletes perform and to help create new and better products. You can change your choice anytime in Settings. Learn More.

Use My Workout Info

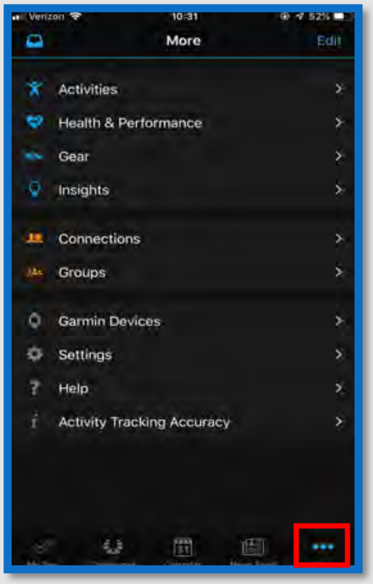
Fitness trackers have gained popularity. Strava has 42 million users and FitBit has 27 million. Neither has had a major data breach yet, but Under Armour did in 2018.

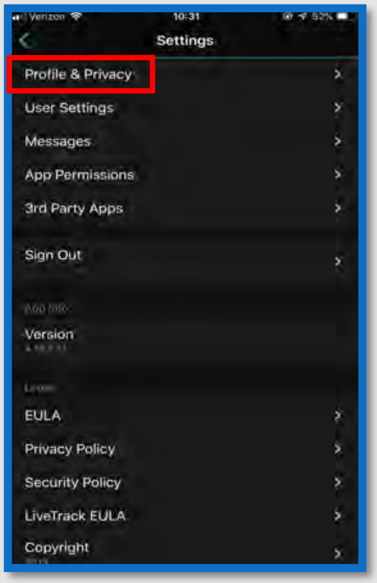
Fitness Apps

Mobile Device Version

*** This information describes how to make your account secure on Android and iPhone mobile devices. Differences between iPhone Operating System (iOS) and Android Operating System (AOS) are minimal, in such cases iPhone images are outlined **blue** and Android **black**.*

Garmin



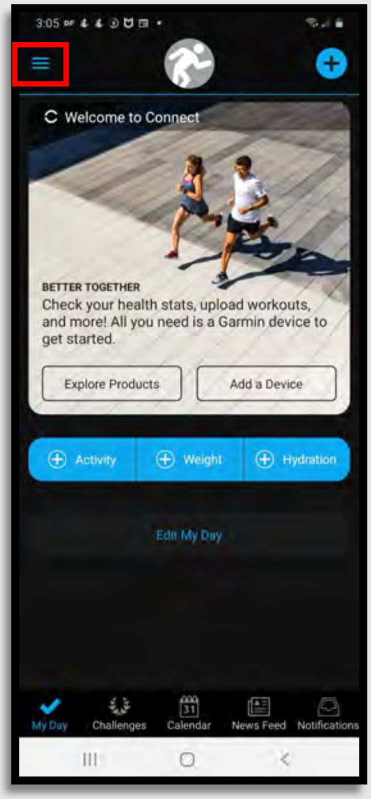


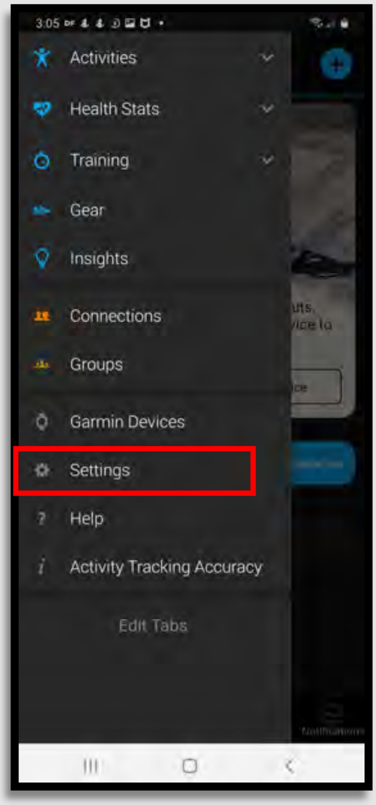
The “Garmin Connect” fitness app is another popular exercise tracker that is capable of sharing a lot of personal information you may not be aware of. If the settings are not set correctly, Garmin will automatically share your information with the public.

First, let’s lock down your “Profile” so that you limit which people can see what kinds of information about you.

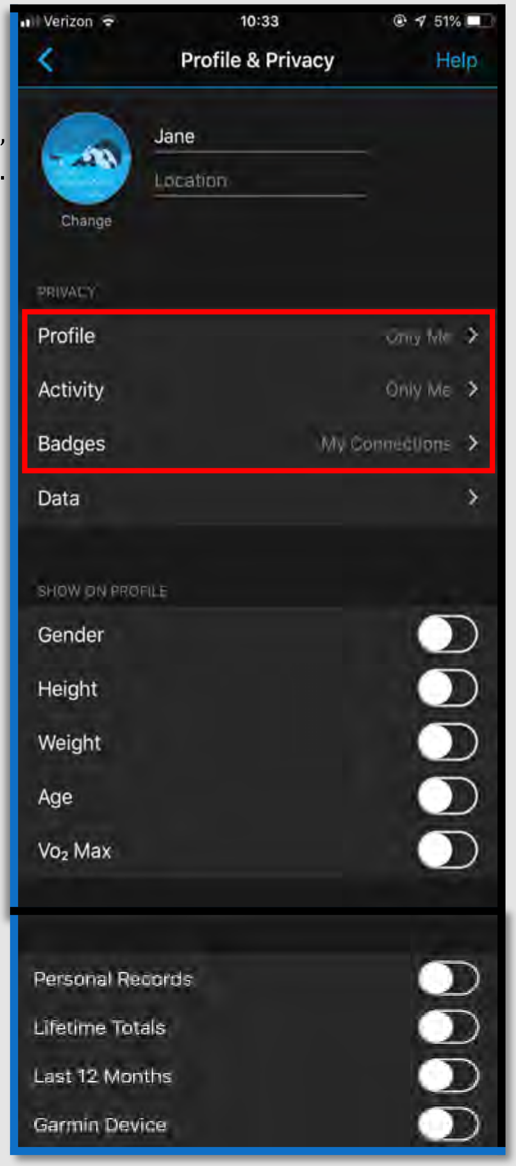
On iPhone: from the “Home” screen, select “More” tab, then select “Settings”, then “Profile & Privacy”. (see left)

On Android: from the “Home” screen, select the “Menu” tab in the top left corner, then select “Settings” toward the bottom of the menu list, select “Profile & Privacy”.





Once in the “Profile & Privacy” section, look through all the privacy settings (see right). We recommend that the tabs in this section be set to "Only Me" or "My Connections." Here you can also choose what personal information you want published on your profile for others to see.



PRIVACY

Profile: Only Me

Activity: Only Me

Badges: My Connections

Data

SHOW ON PROFILE

Gender ○

Height ○

Weight ○

Age ○

VO_2 Max ○

Personal Records ○

Lifetime Totals ○

Last 12 Months ○

Garmin Device ○

Connecting with friends on fitness apps means that you must be concerned with their privacy settings as well as yours.

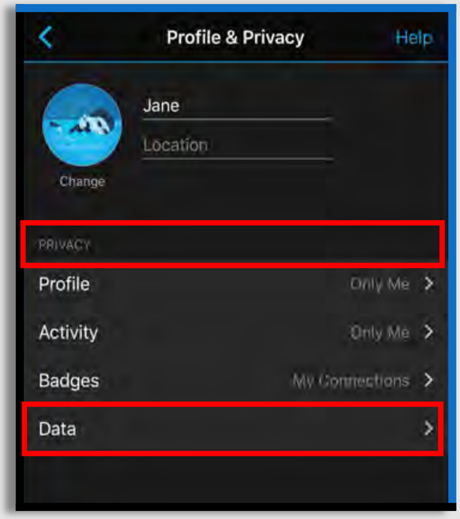
UPDATED JAN 2021

Fitness Apps

Mobile Device Version

*** This information describes how to make your account secure on Android and iPhone mobile devices. Differences between iPhone Operating System (iOS) and Android Operating System (AOS) are minimal, in such cases iPhone images are outlined* ***blue*** *and Android* ***black****.*

Garmin



Profile & Privacy

Help

Jane

Location

Change

PRIVACY

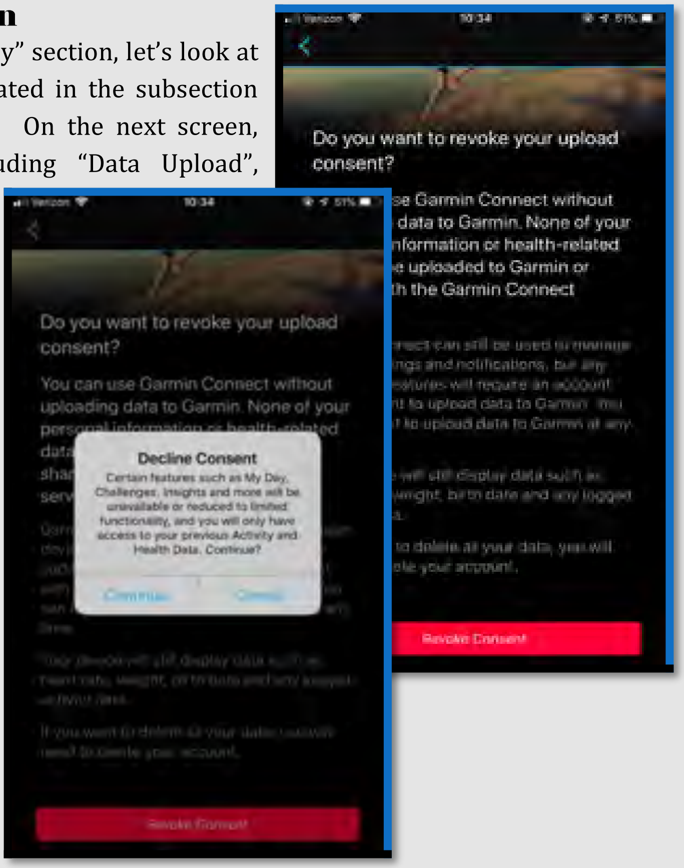
Profile — Only Me

Activity — Only Me

Badges — My Connections

Data

Also, in the "Profile & Privacy" section, let's look at the "Data" section. It is located in the subsection labeled "Privacy" (see left). On the next screen, you will see a list including "Data Upload", "Insights", and "Popularity Routing". First, select "Popularity Routing". This function allows Garmin to collect data from your account and device in order to build and reinforce databases that hold popular routes. We recommend you turn this function off by setting the toggle to "Off". Next, select "Insights" and read through the consent policy provided before you decide if you want to "Agree" or "Do Not Agree", this is your choice. Finally, select "Device Upload" and decide whether you want to Garmin to connect your Garmin devices to "Garmin Connect", set the toggle to "On" or "Off" based on your preference here.



Do you want to revoke your upload consent?

You can use Garmin Connect without uploading data to Garmin. None of your personal information or health-related data ...

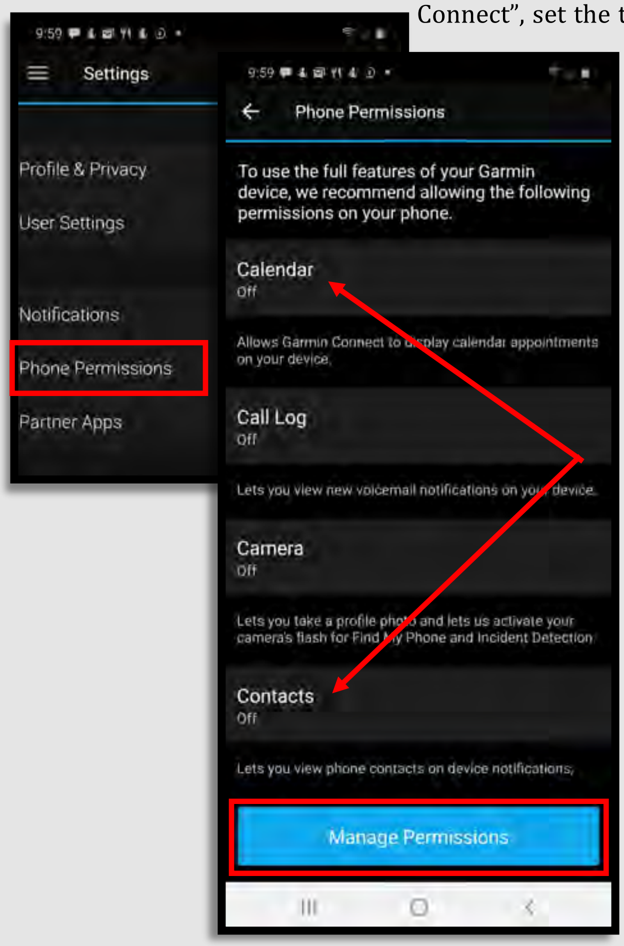
Decline Consent

Certain features such as My Day, Challenges, Insights and more will be unavailable or reduced to limited functionality, and you will only have access to your previous Activity and Health Data. Continue?

Continue — Cancel

If you want to delete all your data, you will need to delete your account.

Revoke Consent



Settings

Profile & Privacy

User Settings

Notifications

Phone Permissions

Partner Apps

Phone Permissions

To use the full features of your Garmin device, we recommend allowing the following permissions on your phone.

Calendar — Off

Allows Garmin Connect to display calendar appointments on your device.

Call Log — Off

Lets you view new voicemail notifications on your device.

Camera — Off

Lets you take a profile photo and lets us activate your camera's flash for Find My Phone and Incident Detection.

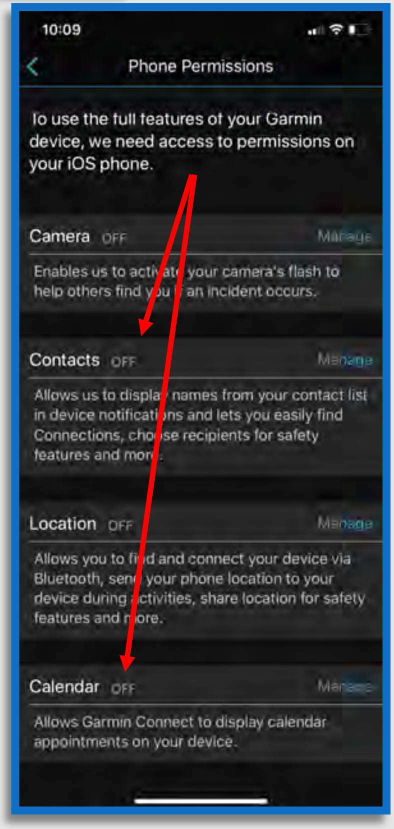
Contacts — Off

Lets you view phone contacts on device notifications.

Manage Permissions

Finally, let's look at what other features of your phone you are letting Garmin have access to. Go back to "Settings", select "Phone "Permissions" and review which device features Garmin is connected to. We recommend you set both "Contacts" and "Calendar" to "Off", and we suggest you consider doing the same for "Camera" and "Location". (see left for Android, and right for iPhone).

On Android: Note that "Location" is further down the list, reference screen shot left.



10:09

Phone Permissions

To use the full features of your Garmin device, we need access to permissions on your iOS phone.

Camera — OFF — Manage

Enables us to activate your camera's flash to help others find you if an incident occurs.

Contacts — OFF — Manage

Allows us to display names from your contact list in device notifications and lets you easily find Connections, choose recipients for safety features and more.

Location — OFF — Manage

Allows you to find and connect your device via Bluetooth, send your phone location to your device during activities, share location for safety features and more.

Calendar — OFF — Manage

Allows Garmin Connect to display calendar appointments on your device.

U.S. health privacy law, known as HIPPA, does not apply to info customers collect for their own use. Therefore, fitness apps don't fall under HIPPA regulations.

UPDATED JAN 2021

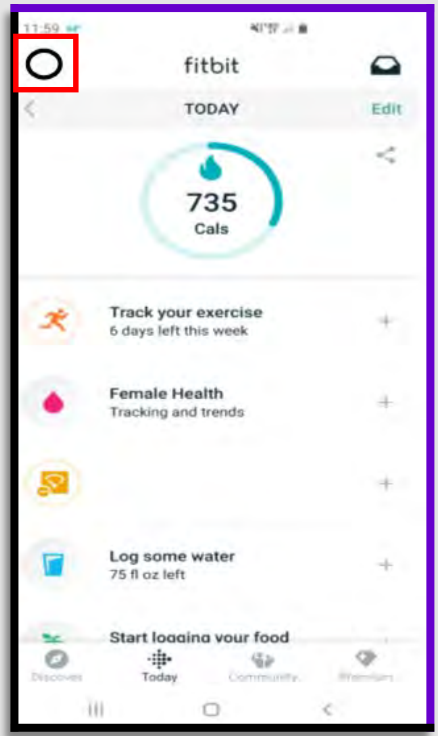
Fitness Apps

Mobile Device Version

*** This information describes how to make your account secure on Android and iPhone mobile devices. Differences between iPhone Operating System (iOS) and Android Operating System (AOS) are minimal, in such cases iPhone images are outlined **purple** and Android **black**.*

Fitbit

FitBit is another popular activity tracker, and one of the first of its kind. Older versions of FitBit were designed to automatically publish workout statistics and information to the public, but newer versions have changed default settings to keep this information private. Therefore, unless you configure it otherwise, your privacy setting *should* be set by default to "Private". Nevertheless, we recommend you always confirm settings yourself.



fitbit

TODAY Edit

735 Cals

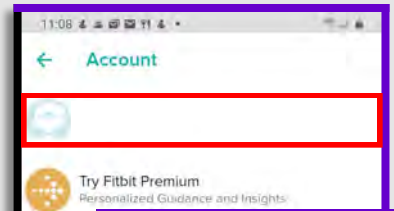
Track your exercise
6 days left this week

Female Health
Tracking and trends

Log some water
75 fl oz left

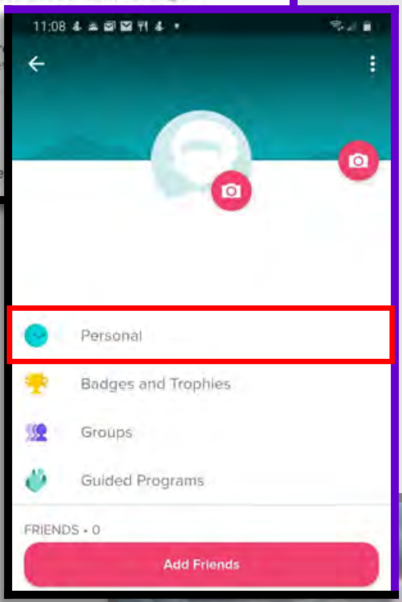
Start logging your food

First, let's review your "Profile" information. From your "Home" screen (see left), select your "Profile Picture" icon in the top left corner. Then select your "Account", noted by your name, and your "Profile Page" will appear, select "Personal" and ensure that "Location" is not turned on. Also review the personal data you have provided to Fitbit on this page. Next, go back to the "Account" section (where you selected your "Account" by name earlier). Here you can review each of your FitBit settings and then head to the "Privacy and Security" section where you will want to pay special attention to each setting.



Account

Try Fitbit Premium
Personalized Guidance and Insights



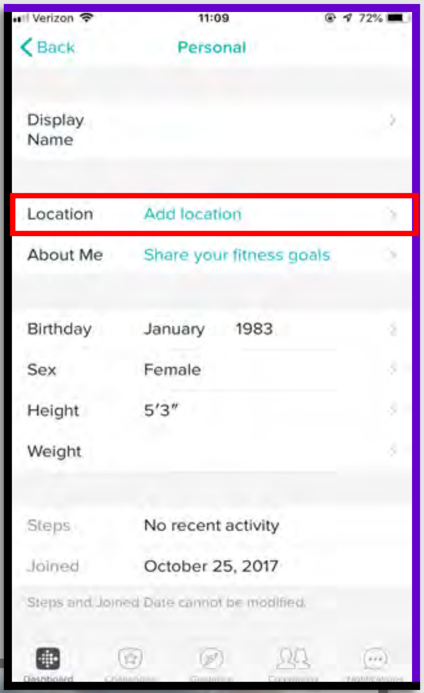
Personal

Badges and Trophies

Groups

Guided Programs

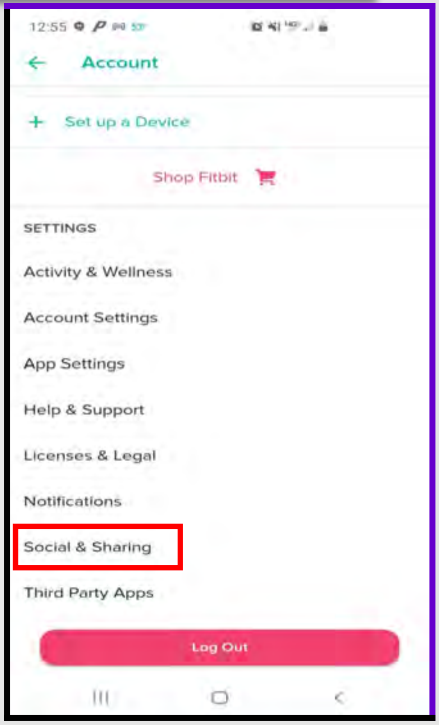
FRIENDS • 0



Back Personal

Display Name	
Location	Add location
About Me	Share your fitness goals
Birthday	January 1983
Sex	Female
Height	5'3"
Weight	
Steps	No recent activity
Joined	October 25, 2017

Steps and Joined Date cannot be modified.



Account

+ Set up a Device

Shop Fitbit

SETTINGS

Activity & Wellness

Account Settings

App Settings

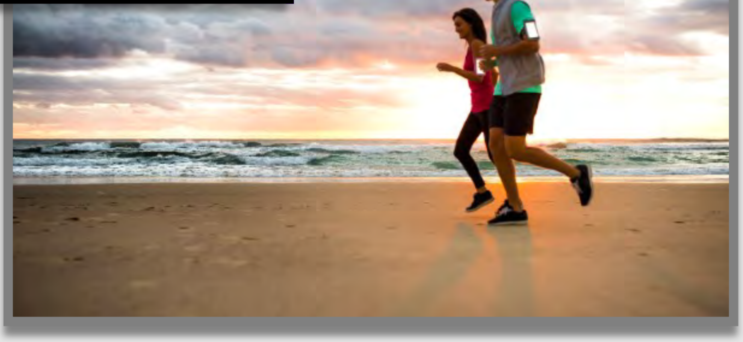
Help & Support

Licenses & Legal

Notifications

Social & Sharing

Third Party Apps



Anytime your fitness app has an update it is a good idea to use this time to also update your password.

UPDATED JAN 2021

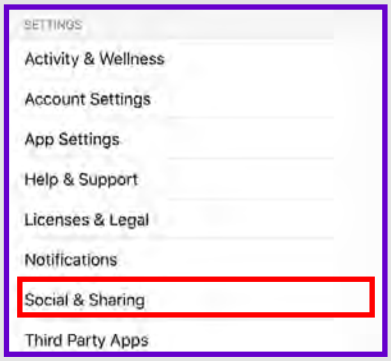
Fitness Apps

Mobile Device Version

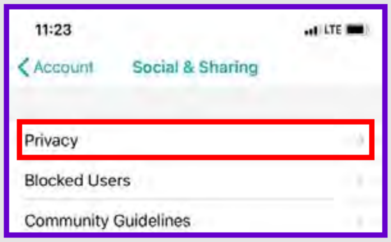
*** This information describes how to make your account secure on Android and iPhone mobile devices. Differences between iPhone Operating System (iOS) and Android Operating System (AOS) are minimal, in such cases iPhone images are outlined **purple** and Android **black**.*

Don't just set the settings within the fitness app, make sure you go into your phone settings and update what you allow for each app from your phone.

Who can see my information?



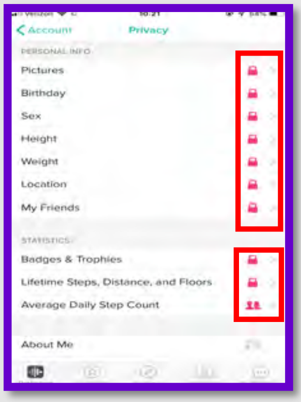
SETTINGS
Activity & Wellness
Account Settings
App Settings
Help & Support
Licenses & Legal
Notifications
Social & Sharing
Third Party Apps



11:23
< Account — Social & Sharing
Privacy
Blocked Users
Community Guidelines

On iPhone: In the “Account” section, select “Social & Sharing” then select the “Privacy” section.

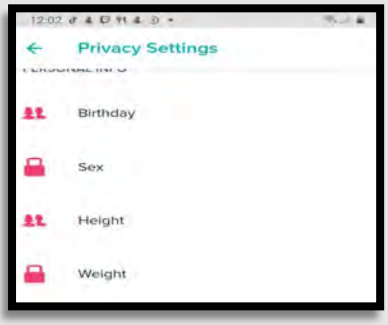
On Android: In the “Account” section, under “Privacy & Security” select “Privacy” to begin locking down your Fitbit.



< Account — Privacy
PERSONAL INFO
Pictures
Birthday
Sex
Height
Weight
Location
My Friends
STATISTICS
Badges & Trophies
Lifetime Steps, Distance, and Floors
Average Daily Step Count
About Me

We recommend that you avoid sharing any information that would be considered “Personally Identifiable Information”, or PII. This is any information connected with your personal identity, including your name, birthday, social security number, etc. To change the setting:

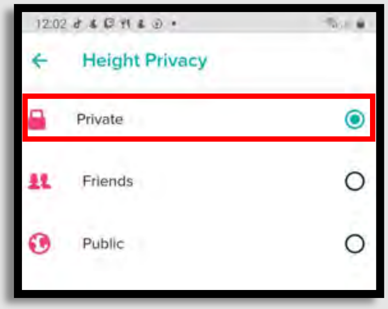
On iPhone: (see left) select the icon to the right of the category, for instance the “Private” icon is a padlock, “Friends” is an image of two people, and “Public” is represented by a globe. Select the icon and make the change, then select “Save” in the upper right corner of the screen.



12:02
← Privacy Settings
PERSONAL INFO
Birthday
Sex
Height
Weight

On Android: select the category itself, make the change, and select the back arrow. The change is automatically saved.

Important Note: The “About Me” section, located toward the bottom of the “Privacy” page, is always set to “Public”. You cannot control this feature, as indicated by its greyed out appearance. You write your “About Me” information in your “Profile” section. The image to the right is for iPhone only, and this section is not available on Android.



12:02
← Height Privacy
Private ●
Friends ○
Public ○

Finally, go back to the “Account” section and review the “Manage Data” section where you can delete or limit what third party apps have access to your Fitbit and vice versa. (not shown)

Polar Flow

Polar is a company that produces fitness tracking watches and hardware, all of which connect to its popular app, Polar Flow. According to a recent investigation, the app's tracking map exposed the home addresses of thousands of users. This is in part because people often turn their fitness trackers “On” or “Off” when they're close to home, unintentionally revealing where they live.

To keep your data private on Polar Flow:

- Go to “Settings” and then “Privacy”, and set the default to “Private”
- Change the privacy of each of your past runs individually, set them each to “Private”
- Set your “Profile” to “Private”

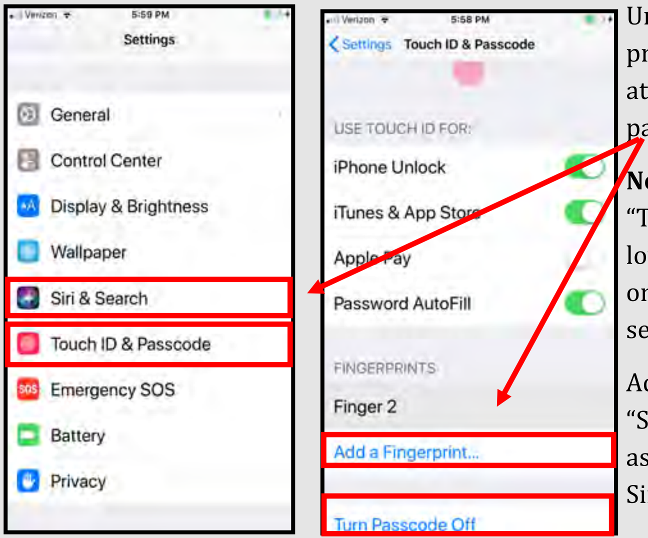
UPDATED JAN 2021

iOS PRIVACY SETTINGS (iOS 14.1) SMART CARD

“Best Practices”

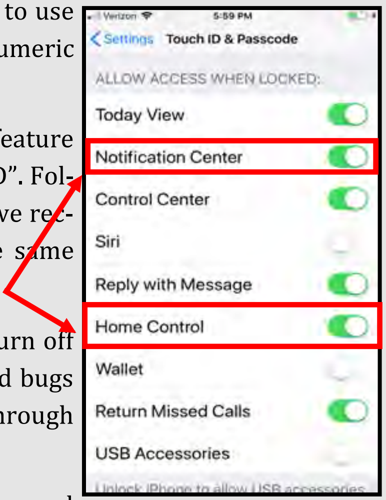
- Smartphones and tablets are not impenetrable. Secure your smartphone with a password, and use apps such as “Find My iPhone” to locate lost or stolen devices.
- All smartphones and tablets have cameras and microphones that can be remotely activated. Caution should be used when device is near anything of personal importance.
- Bluetooth and wireless capable devices are convenient but easily exploitable by hackers. Use a VPN if possible and avoid public wireless networks. It is advisable to turn these services off if not immediately needed.
- Prior to downloading apps on your device, read the developers permissions. Many apps require permission to access your camera, microphone, text messages, and contacts.
- Turn off location services until they are actually needed. Otherwise, your daily movements may be tracked by various apps and vendors. Whether turned on or off, location services are always available to 911 and first responders.

“Physical Security”



Verizon 5:59 PM
Settings
General
Control Center
Display & Brightness
Wallpaper
Siri & Search
Touch ID & Passcode
Emergency SOS
Battery
Privacy

Verizon 5:58 PM
Settings Touch ID & Passcode
USE TOUCH ID FOR:
iPhone Unlock
iTunes & App Store
Apple Pay
Password AutoFill
FINGERPRINTS
Finger 2
Add a Fingerprint...
Turn Passcode Off



Verizon 5:59 PM
Settings Touch ID & Passcode
ALLOW ACCESS WHEN LOCKED:
Today View
Notification Center
Control Center
Siri
Reply with Message
Home Control
Wallet
Return Missed Calls
USB Accessories
Unlock iPhone to allow USB accessories

Under “Settings” and “ Touch/Face ID & Passcode,” select “Add a Fingerprint” and “Turn Passcode On”. Be sure to use at least a 6 digit passcode. Alpha-numeric passcodes are even better options.

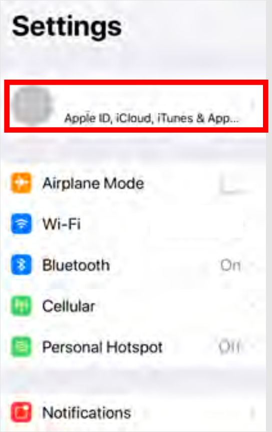
Note: iPhone 11 has taken off the feature “Touch ID” and replaced it with “Face ID”. Follow directions to create a Face ID, and we recommend under “Use Face ID For”, the same settings as “Use Touch ID For” (left)

Additionally, we recommend that you turn off “Siri” due to its listening capabilities and bugs associated with accessing your phone through Siri without a password.

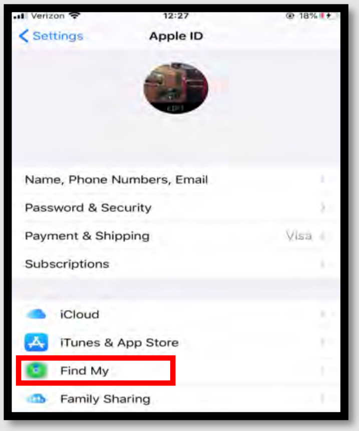
Finally, scroll further down in this section, and we recommend setting the functions under “Allow Access When Locked”, as seen here (above right), in order to limit access.

“Find My iPhone”

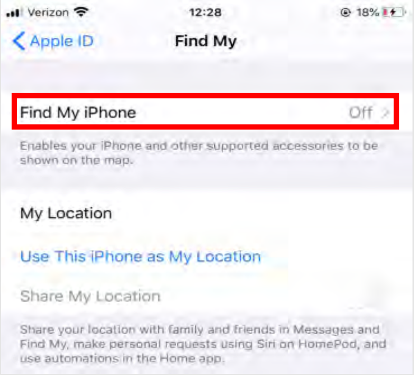
Next go to “Settings” and select your account at the top (highlighted in **red** to the right). From there, select “Find My,” then select “Find My iPhone” and ensure it is turned “On”. This way if you lose your phone, you can access your account online and geo-locate where it is.



Settings
Apple ID, iCloud, iTunes & App...
Airplane Mode
Wi-Fi
Bluetooth On
Cellular
Personal Hotspot Off
Notifications



Verizon 12:27 18%
Settings Apple ID
Name, Phone Numbers, Email
Password & Security
Payment & Shipping Visa
Subscriptions
iCloud
iTunes & App Store
Find My
Family Sharing



Verizon 12:28 18%
Apple ID Find My
Find My iPhone Off
Enables your iPhone and other supported accessories to be shown on the map.
My Location
Use This iPhone as My Location
Share My Location
Share your location with family and friends in Messages and Find My, make personal requests using Siri on HomePod, and use automations in the Home app.

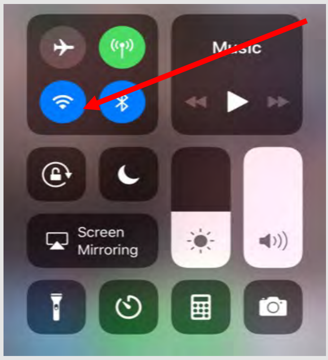
Smartphones contain extremely sensitive personal data and therefore should be treated with extra security precautions #protectyourdata

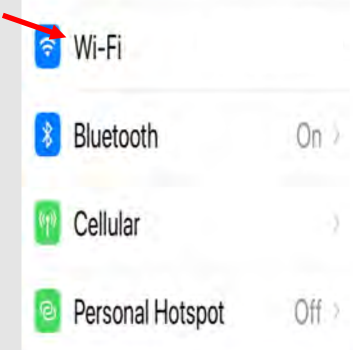
UPDATED JAN 2021

iOS PRIVACY SETTINGS (iOS 14.1) SMART CARD

"Wireless Networks"

Where possible, public WIFI networks should be avoided due to the vulnerabilities they present to your personal data. If public networks must be used, avoid logging into accounts that require passwords and always use a VPN client to encrypt on-line transactions. There are two ways to turn off WIFI: 1) Scroll up from the bottom of your phone and tap the icon on the control screen; or 2) In "Settings", Select "WIFI", and it turn off.



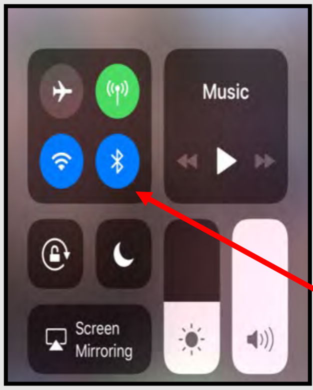

Wi-Fi

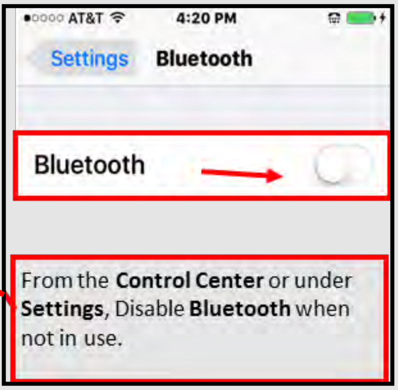
Bluetooth On

Cellular

Personal Hotspot Off

"Bluetooth"





Bluetooth

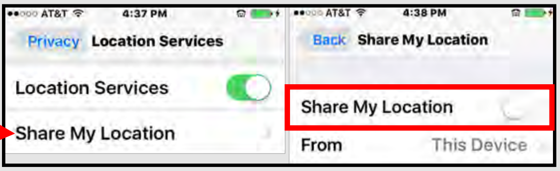
From the **Control Center** or under **Settings**, Disable **Bluetooth** when not in use.

Bluetooth is a wireless technology standard for exchanging data over short distances from fixed and mobile devices. When Bluetooth is enabled on your iPhone or tablet, hackers can gain access to your device and obtain contacts, messages, calendars, photos, and notes without your knowledge. It is therefore recommended that you only use Bluetooth when necessary, like in your car, and that you turn it off after you are done using it each time.

"Location Services"

Whenever you take a photo, your phone records the location and saves that information inside the photo's EXIF data. When you send that photo to someone else, they may be able to see where you took it, in some cases, down to a specific street. If you post a picture taken from your home, anyone who can view the EXIF data could figure out where you live and more. It is important to remove the EXIF data, or better yet prevent your devices from including it in pictures. Please refer to the "EXIF" Smartcard in this book for information on how to do this.

To disable your location from being shared in "Message "and "Find my Friends", open the "Settings" app and navigate to "Privacy" > "Location Services." Then navigate to "Share My Location" and tap on the toggle to disable "Share My Location."

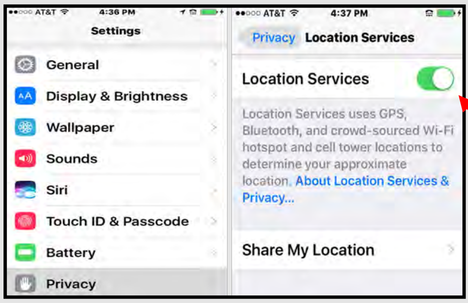


Location Services

Share My Location

Share My Location

From This Device

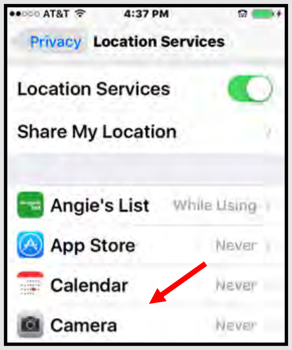


Location Services

Location Services uses GPS, Bluetooth, and crowd-sourced Wi-Fi hotspot and cell tower locations to determine your approximate location. About Location Services & Privacy...

Share My Location

Note: If you turn off "Location Services" in the "Privacy Setting "menu, you cannot use location services for things such as "Navigation" or "Find My iPhone" if lost or stolen. You can still wipe your phone, using the "Find My iPhone", if "Location Services" are off. "Alternatively, you can leave "Location Services" on in "Privacy Settings" but turn it off for installed apps you don't want to have access. Just scroll down to find which apps use your location.

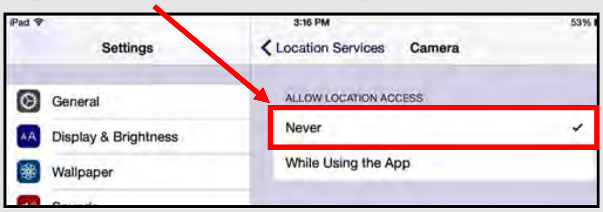


Location Services

Share My Location

Angie's List	While Using
App Store	Never
Calendar	Never
Camera	Never

Go back to "Location Services" to disable your location from being saved with photos, and tap on "Camera" to change this setting. Note: The "Location Services" toggle must be on to find the camera option. Perform the same steps to disable location services for other apps listed in the "Location Services" setting. Navigation and maps apps are examples of those that require "Location Services. "



ALLOW LOCATION ACCESS

Never ✓

While Using the App

Leaving location settings on can give someone a pattern of life for you and your family. #turnitoff

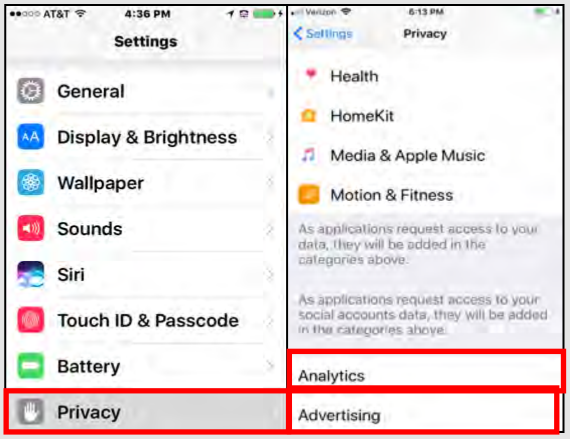
UPDATED JAN 2021

iOS PRIVACY SETTINGS (iOS 14.1) SMART CARD

“Analytics Data and Ad Tracking”

“Analytics” enables a feature that gives Apple permission to track your activities. “Ad Tracking” allows vendors to send ads to you, targeted to your interests. Apple provides a setting to allow you to opt out of both of these features. It is recommended that you turn off “Ad Tracking.”

1) Open up the “Settings” app and navigate to “Privacy” then to “Analytics” and “Advertising”



●●○○○ AT&T 4:36 PM

Settings

General
Display & Brightness
Wallpaper
Sounds
Siri
Touch ID & Passcode
Battery
Privacy

Verizon 6:13 PM

< Settings Privacy

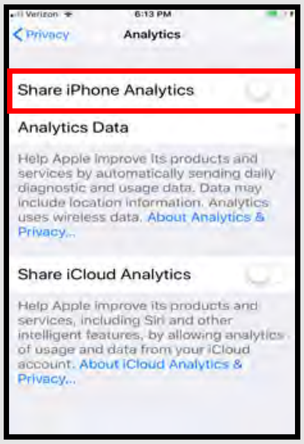
Health
HomeKit
Media & Apple Music
Motion & Fitness

As applications request access to your data, they will be added in the categories above.

As applications request access to your social accounts data, they will be added in the categories above.

Analytics
Advertising

2) Select “Analytics” and Then turn off “Share iPhone Analytics”



Verizon 6:13 PM

< Privacy Analytics

Share iPhone Analytics

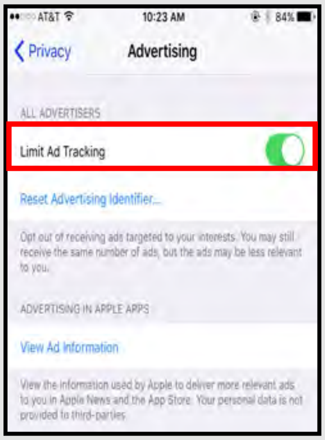
Analytics Data

Help Apple improve its products and services by automatically sending daily diagnostic and usage data. Data may include location information. Analytics uses wireless data. About Analytics & Privacy...

Share iCloud Analytics

Help Apple improve its products and services, including Siri and other intelligent features, by allowing analytics of usage and data from your iCloud account. About iCloud Analytics & Privacy...

3) Then go back and select “Advertising” Turn ON “Limit Ad Tracking.”



●●○○○ AT&T 10:23 AM 84%

< Privacy Advertising

ALL ADVERTISERS

Limit Ad Tracking

Reset Advertising Identifier...

Opt out of receiving ads targeted to your interests. You may still receive the same number of ads, but the ads may be less relevant to you.

ADVERTISING IN APPLE APPS

View Ad Information

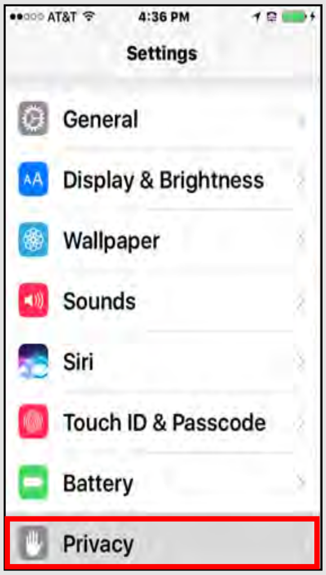
View the information used by Apple to deliver more relevant ads to you in Apple News and the App Store. Your personal data is not provided to third-parties

“Location-Based Apple Ads”

“Apple Ads” allow Apple to serve you with ads, based on your location. “Location-Based Ads” do not use your exact location and Apple does not give this information to advertisers. Here’s how to disable “Apple Ads”:

Open up “Settings” > “Privacy” > “Location Services” > “System Services.” You’ll see a list of location-based selections that can be toggled off.

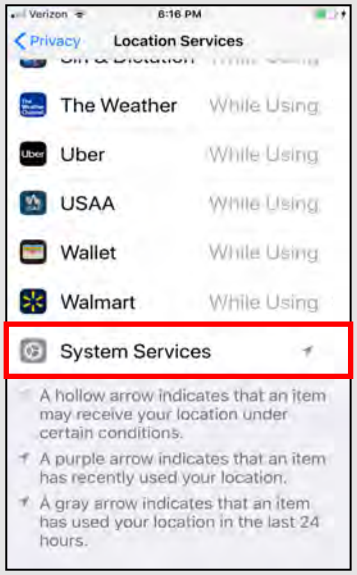
While in “System Services,” it is also recommended you scroll to the lower portion of the screen and select “Significant Locations. From there be sure the “Significant Locations is toggled to the “off” switch, so that your Wi-Fi and iPhone are not capturing your location data.



●●○○○ AT&T 4:36 PM

Settings

General
Display & Brightness
Wallpaper
Sounds
Siri
Touch ID & Passcode
Battery
Privacy



Verizon 6:16 PM

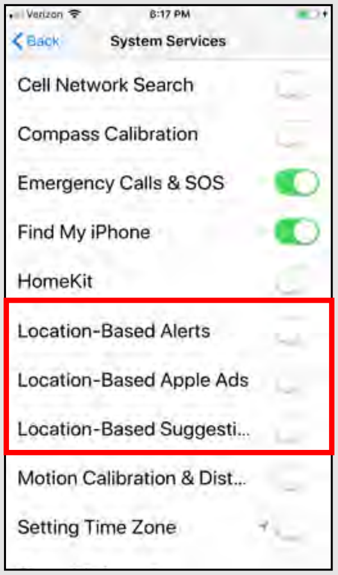
< Privacy Location Services

The Weather While Using
Uber While Using
USAA While Using
Wallet While Using
Walmart While Using
System Services

A hollow arrow indicates that an item may receive your location under certain conditions.

A purple arrow indicates that an item has recently used your location.

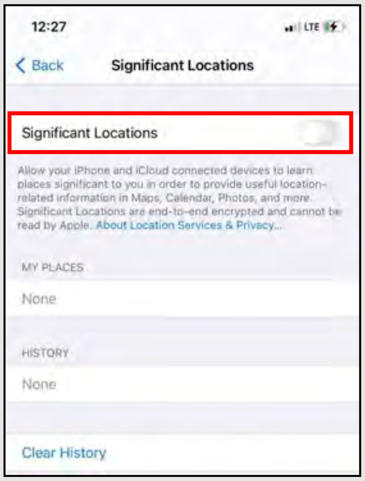
A gray arrow indicates that an item has used your location in the last 24 hours.



Verizon 6:17 PM

< Back System Services

Cell Network Search
Compass Calibration
Emergency Calls & SOS
Find My iPhone
HomeKit
Location-Based Alerts
Location-Based Apple Ads
Location-Based Suggesti...
Motion Calibration & Dist...
Setting Time Zone



12:27 LTE

< Back Significant Locations

Significant Locations

Allow your iPhone and iCloud connected devices to learn places significant to you in order to provide useful location-related information in Maps, Calendar, Photos, and more. Significant Locations are end-to-end encrypted and cannot be read by Apple. About Location Services & Privacy...

MY PLACES

None

HISTORY

None

Clear History

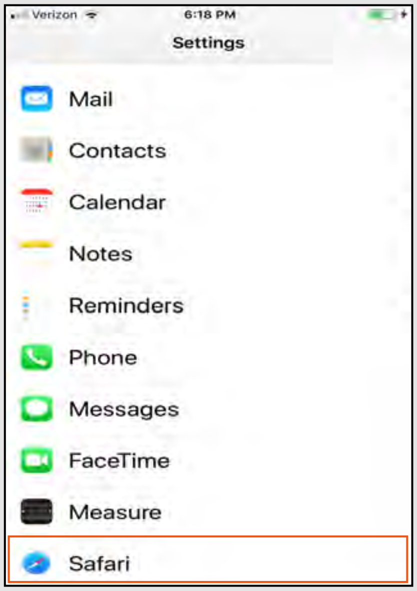
Marketing data is not just available to marketing companies anymore. #turnadsoff

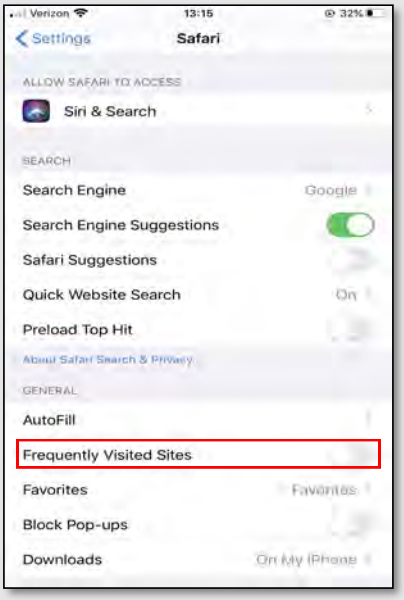
UPDATED JAN 2021

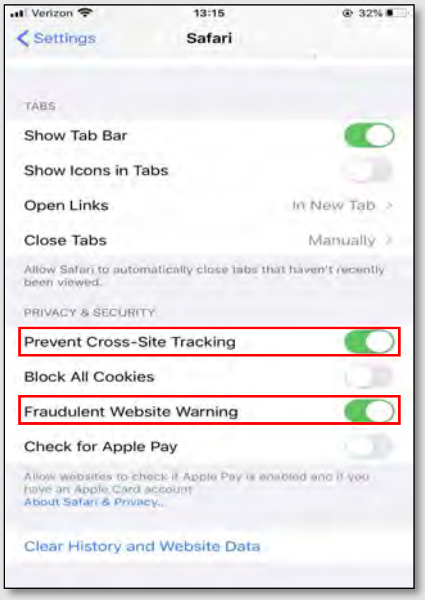
iOS PRIVACY SETTINGS (iOS 14.1) SMART CARD

Safari's "Do Not Track"

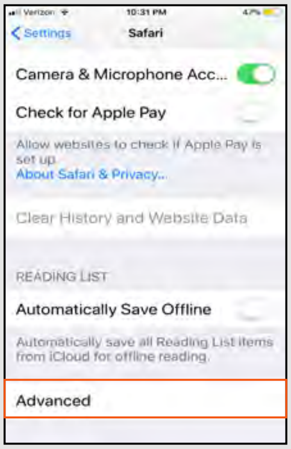
Safari's "Do Not Track" is a universal web tracking opt-out initiative that allows users to prevent advertisers from tracking your browsing habits. The Safari browser on iOS 13.0 allows users to opt-out to prevent advertisers from seeing users mobile web browsing history. To opt-out, open the "Settings" app, scroll down and select "Safari". There are several sections to look through and adjust the settings, but definitely turn off "Frequently Visited Sites" under the section titled "General". This prevents Safari from tracking sites you regularly visit. Next, under the "Privacy & Security" section on the "Safari" page, turn on "Prevent Cross-Site Tracking" and "Fraudulent Website Warning."

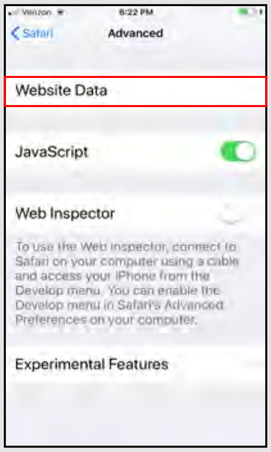

Verizon 6:18 PM
Settings
Mail
Contacts
Calendar
Notes
Reminders
Phone
Messages
FaceTime
Measure
Safari

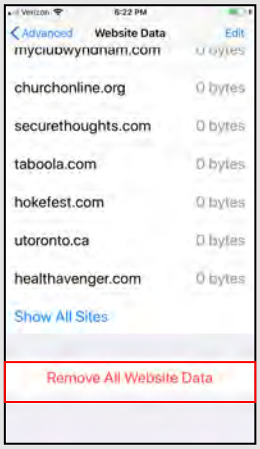

Verizon 13:15 32%
Settings Safari
ALLOW SAFARI TO ACCESS
Siri & Search
SEARCH
Search Engine Google
Search Engine Suggestions
Safari Suggestions
Quick Website Search On
Preload Top Hit
About Safari Search & Privacy...
GENERAL
AutoFill
Frequently Visited Sites
Favorites Favorites
Block Pop-ups
Downloads On My iPhone


Verizon 13:15 32%
Settings Safari
TABS
Show Tab Bar
Show Icons in Tabs
Open Links In New Tab
Close Tabs Manually
Allow Safari to automatically close tabs that haven't recently been viewed.
PRIVACY & SECURITY
Prevent Cross-Site Tracking
Block All Cookies
Fraudulent Website Warning
Check for Apple Pay
Allow websites to check if Apple Pay is enabled and if you have an Apple Card account.
About Safari & Privacy...
Clear History and Website Data

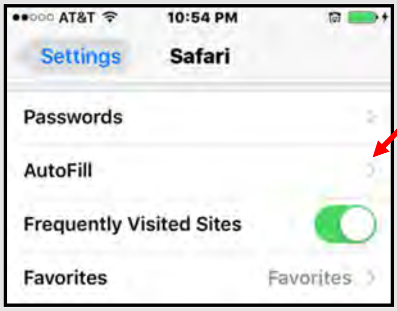
It is also a best practice to clear the browser history periodically. To do so, continue to scroll down in the Safari settings, at the very bottom select "Advanced" > "Website Data", then select "Remove All Website Data"


Verizon 10:31 PM 47%
Settings Safari
Camera & Microphone Acc...
Check for Apple Pay
Allow websites to check if Apple Pay is set up.
About Safari & Privacy...
Clear History and Website Data
READING LIST
Automatically Save Offline
Automatically save all Reading List items from iCloud for offline reading.
Advanced


Verizon 6:22 PM
Safari Advanced
Website Data
JavaScript
Web Inspector
To use the Web Inspector, connect to Safari on your computer using a cable and access your iPhone from the Develop menu. You can enable the Develop menu in Safari's Advanced Preferences on your computer.
Experimental Features

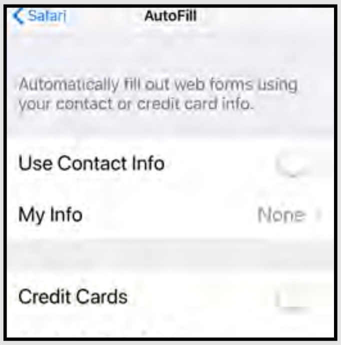

Verizon 6:22 PM
Advanced Website Data Edit
myclubwyndham.com 0 bytes
churchonline.org 0 bytes
securethoughts.com 0 bytes
taboola.com 0 bytes
hokefest.com 0 bytes
utoronto.ca 0 bytes
healthavenger.com 0 bytes
Show All Sites
Remove All Website Data

"Passwords and AutoFill"


AT&T 10:54 PM
Settings Safari
Passwords
AutoFill
Frequently Visited Sites
Favorites Favorites

Clear the AutoFill to protect passwords and credit card information. To do so, open "Settings" > "Safari" and click on "AutoFill"

Next, select the following settings to disable "Use Contact Info", and "Credit Cards"


Safari AutoFill
Automatically fill out web forms using your contact or credit card info.
Use Contact Info
My Info None
Credit Cards

Google already tracks everything we do, so why let another search engine do it too? #saynototracking

UPDATED JAN 2021

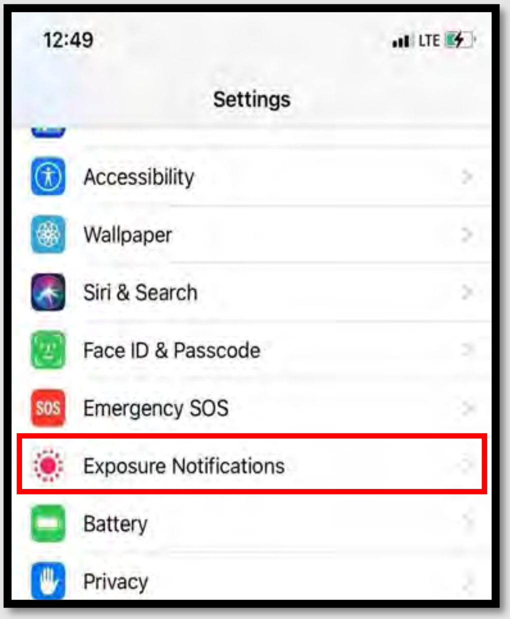
iOS PRIVACY SETTINGS (iOS 14.1) SMART CARD

The Covid-19 Exposure Tracking System will be opt-in on your iPhone. It will require an additional download from your local health system in order to work.

COVID 19 Contact Tracing

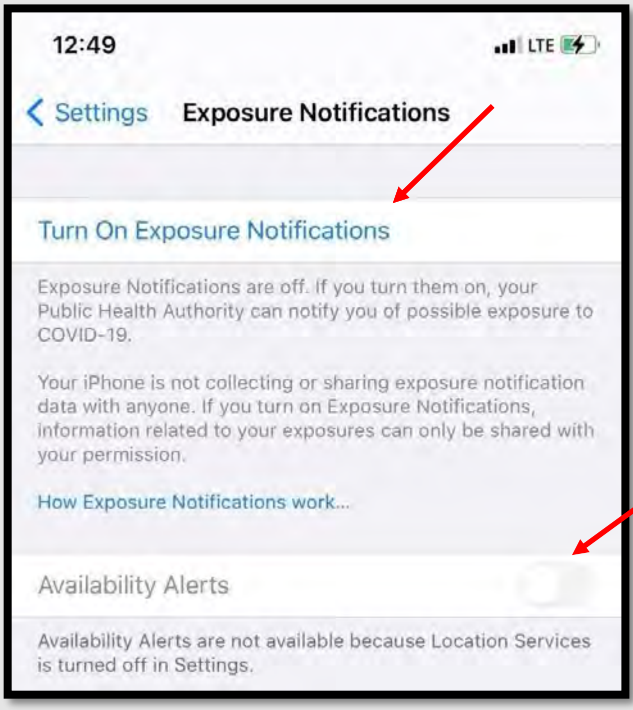
Apple and Google have partnered on offering a secure and private coronavirus contact tracing implementation on iOS and Android. Contact tracing is called "Exposure Notifications" on iPhone, and is default set to "Off". You'll have to download an app from your local health authority that will require your explicit permission to use anonymous Bluetooth data for it to work, upon rollout of the system in May 2020. Later in the year 2020, contact tracing software will allow it to work without a third-party health authority app.

In the meantime, you may be curious as to status of the "Exposure Logging" function on your iPhone. You can see whether yours is activated by going to "Settings" > "Exposure Notifications" > "Exposure Logging". When you see "Exposure Logging", you will notice a toggle to the right that is probably "Off". You can attempt to turn it "On", and if you aren't able to do so, then the tool is not yet active on your iPhone.


12:49

Settings

- Accessibility
- Wallpaper
- Siri & Search
- Face ID & Passcode
- Emergency SOS
- Exposure Notifications
- Battery
- Privacy


12:49

< Settings   Exposure Notifications

Turn On Exposure Notifications

Exposure Notifications are off. If you turn them on, your Public Health Authority can notify you of possible exposure to COVID-19.

Your iPhone is not collecting or sharing exposure notification data with anyone. If you turn on Exposure Notifications, information related to your exposures can only be shared with your permission.

How Exposure Notifications work...

Availability Alerts

Availability Alerts are not available because Location Services is turned off in Settings.

If you decide at any point that you want to disable the "Exposure Notifications Logging" tool on your iPhone, you can take the following steps. First, on iOS 13.5 and later, go to "Settings" on your iPhone. Next, swipe down and select "Exposure Notifications". For now, you'll need an authorized app before "Exposure Notifications" can be turned on, but when that happens you can tap the toggle to turn notifications "On" or "Off". You can also delete the exposure logs manually at any time by going to the bottom of the "Exposure Logging" page and selecting "Delete Exposure Log". (see above)

If you have opted-in to the "Exposure Logging" system, you may be interested to know who is trying to access your exposure information. To find out, select "Exposure Checks" on the "Exposure Logging" page. This is a record of all requests to check your "Exposure Log" from the past 14 days.

Note: The "Exposure Logging" toggle is disabled by default in iOS 14.1. It does not connect any data without you installing and authorizing a local health authority app, which will be available soon. Apple and Google's exposure notification system will be completely opt-in.

UPDATED JAN 2021

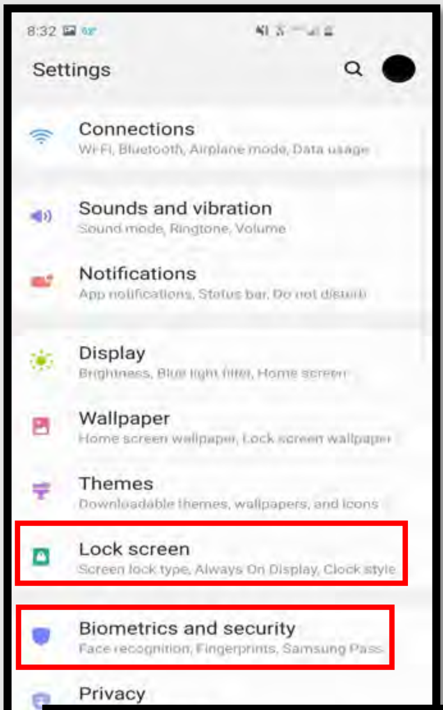
ANDROID PRIVACY SETTINGS (ANDROID 10.0)

Best Practices

- Smartphones and tablets are not impenetrable. Secure your smartphone with a password or biometrics, and utilize apps such as **Find My Device** or **Prey Anti Theft** to locate lost or stolen devices.
- All smartphones and tablets have cameras and microphones that can be remotely activated. Consider your device when you are in certain places or conversations.
- Bluetooth and wireless capable devices are convenient but easily exploitable by hackers. Use a VPN if possible, and always avoid public wireless networks.
- Prior to downloading apps on your device, read the developer's permissions. Many apps request permission to access your camera, microphone, text messages, and phone contacts.
- Keep location services turned off until they are actually needed. Otherwise, your daily movements are likely being tracked. Don't worry, location services are always available to 911 and first responders, even when turned off.
- If you have a google account, you can use your google credentials to login at **maps.google.com/locationhistory** to see your device location history for the last year or more.

***NOTE:** Due to varying Android manufacturers, the instructions in this Smart Card may vary slightly depending on the device being used.*

The most important thing you can do to keep your information secure is to keep your device up to date. In order to make sure your Android is up to date with the latest Android Version, first go to "Settings" then "System," scroll to the bottom and select "Advanced." From there you will see the "System Update" tab, select the tab . (On some versions, you may go to "Settings", then "Software update" toward the bottom of the "Settings" list).


8:32
Settings
Connections
Wi-Fi, Bluetooth, Airplane mode, Data usage
Sounds and vibration
Sound mode, Ringtone, Volume
Notifications
App notifications, Status bar, Do not disturb
Display
Brightness, Blue light filter, Home screen
Wallpaper
Home screen wallpaper, Lock screen wallpaper
Themes
Downloadable themes, wallpapers, and icons
Lock screen
Screen lock type, Always On Display, Clock style
Biometrics and security
Face recognition, Fingerprints, Samsung Pass
Privacy

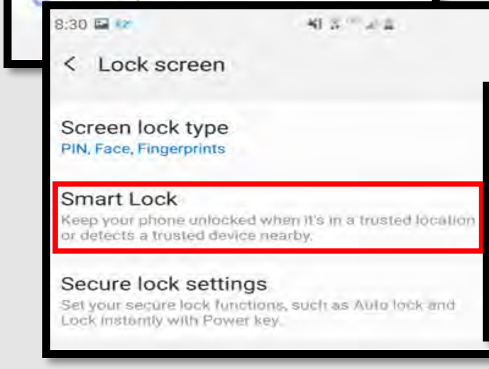
Physical Security

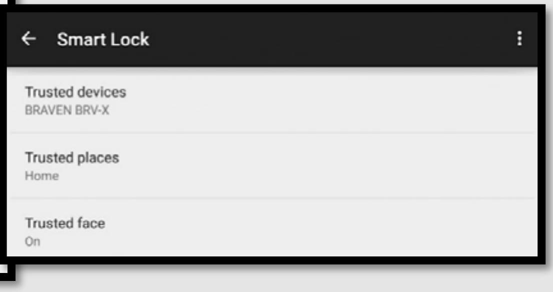
The first line of defense in preventing unauthorized access to your device is to protect it with a "Passcode". In addition, Android 9.0 offers several enhanced security features, including "Fingerprints", "Facial Recognition", "Encryption", and "App-level Permissions".

Under "Settings", first select "Biometrics and security". Here, you can set up your "Face recognition" and "Fingerprints" profiles. You will then go back to "Settings" and select "Lock Screen" in order to set your screen-lock preferences. Tap the "Settings" icon and then tap "Lock Screen." The options are Swipe, Pattern, PIN, Password, Face, Fingerprints. The most secure way to protect your phone is to use the **biometric** options, such as "Face Recognition" and "Fingerprints". A "Password" is the strongest backup solution.

Also under "Lock Screen", you will see the feature "Smart Lock", which allows you to set "Trusted Places" inside of which your device will unlock itself and remain unlocked. This feature can be set to recognize your face and "Trusted Devices" as well, all of which trigger your device to "Unlock" and remain unlocked. This feature is meant for your convenience, but presents obvious vulnerabilities. We recommend you do not enable any "Trusted Features".

Under the "Biometrics & Security" section, you may be able to select the option to "Encrypt Phone", which allows you to initiate the encryption of all data on your device. According to the instructions, this could take up to an hour and requires your device to be plugged into its charger. This process must not be interrupted, so be sure to start it when you are sure you will not need to use your device for that amount of time. You will only need to perform this once. Locking your device encrypts the data on your phone. Unlocking your encrypted device decrypts your data.


8:30
Lock screen
Screen lock type
PIN, Face, Fingerprints
Smart Lock
Keep your phone unlocked when it's in a trusted location or detects a trusted device nearby.
Secure lock settings
Set your secure lock functions, such as Auto lock and Lock instantly with Power key.



Most Androids have a Secure Folder where you can save sensitive documents on your phone with additional password protection.

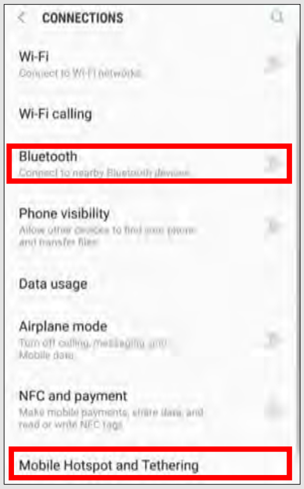
UPDATED JAN 2021

ANDROID PRIVACY SETTINGS (ANDROID 10.0)

Mobile Hotspot, Bluetooth and Wi-Fi

Mobile hotspots devices can be purchased and used for connecting to the internet remotely, but without connecting to public Wi-Fi, which is always discourage. Most Android Smartphones have a "hotspot" feature that allows you to connect to your internet (for instance on your laptop) remotely. By turning on this feature, your phone uses its cellular data to create a "Wi-Fi hotspot". You can turn this option on and off under "Settings" >"Connections" > "Mobile Hotpot and Tethering". **Bluetooth** is a wireless technology for exchanging data over short distances from fixed and mobile devices. When Bluetooth is enabled on your device, hackers could gain entry to your device and obtain contacts, messages, calendars, photos, and notes, or install malware without you even knowing. To disable Bluetooth go to "Settings" > "Connections". When using **Wi-Fi** on your Android it is important to ensure the "Turn on Wi-Fi automatically" feature is turned off. To do this head to the Wi-Fi screen then select "Advanced" in the upper right hand corner. If this function is turned on simply toggle the switch to the "off" position as shown below.

Wireless Networks



CONNECTIONS

Wi-Fi
Connect to Wi-Fi networks

Wi-Fi calling

Bluetooth
Connect to nearby Bluetooth devices

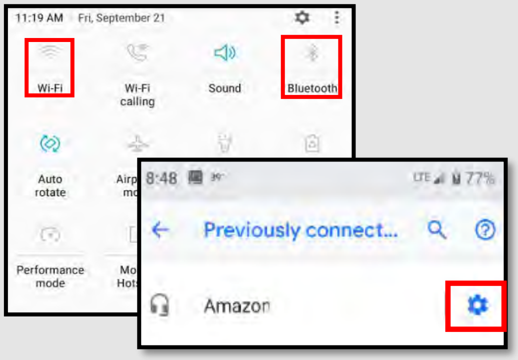
Phone visibility
Allow other devices to find your phone and transfer files

Data usage

Airplane mode
Turn off calling, messaging, and Mobile data

NFC and payment
Make mobile payments, share data, and read or write NFC tags

Mobile Hotspot and Tethering



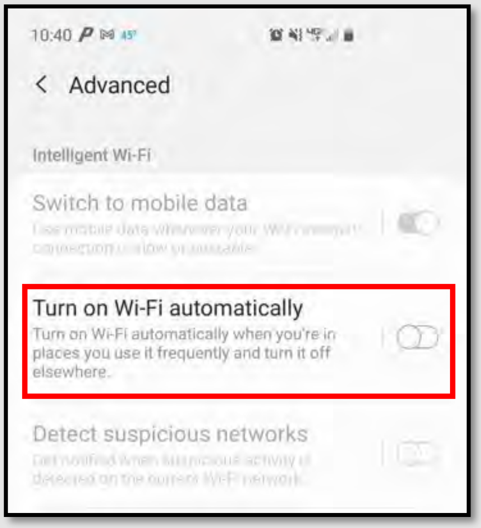
11:19 AM Fri, September 21

Wi-Fi
Wi-Fi calling
Sound
Bluetooth
Auto rotate
Airp mo
Performance mode
Mo Hots

8:48 LTE 77%

Previously connect...

Amazon



10:40

Advanced

Intelligent Wi-Fi

Switch to mobile data
Use mobile data whenever your Wi-Fi internet connection is slow or unstable.

Turn on Wi-Fi automatically
Turn on Wi-Fi automatically when you're in places you use it frequently and turn it off elsewhere.

Detect suspicious networks
Get notified when suspicious activity is detected on the current Wi-Fi network.

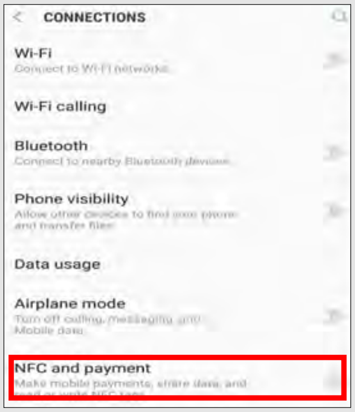
Note: We always recommend avoiding public Wi-Fi networks because they are unsecured. If you must use one, avoid logging into accounts that require passwords and use a VPN client to encrypt on-line transactions.

Note: In order to delete Bluetooth sessions you no longer need, go to "Bluetooth", select "Previously Connected Devices" then select the "Settings" icon, select "Forget."

Near Field Communication (NFC)

NFC is technology that allows you to "bump" your smartphone with other NFC devices to exchange information or pay for items using a Pay app. A malicious user can tamper with the data being transmitted between two NFC devices if they are within range. malware.

Turn off NFC when not in use by tapping "Settings" > "Wireless & Networks" or "Connections". Then tap the toggle switch for "NFC and payment" so that it is in the "off" position.



CONNECTIONS

Wi-Fi
Connect to Wi-Fi networks

Wi-Fi calling

Bluetooth
Connect to nearby Bluetooth devices

Phone visibility
Allow other devices to find your phone and transfer files

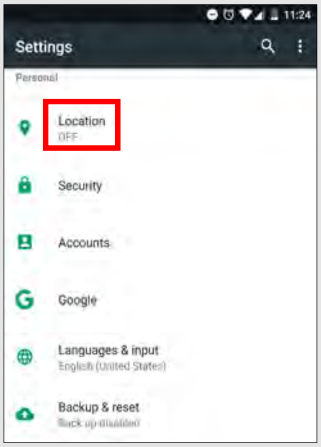
Data usage

Airplane mode
Turn off calling, messaging, and Mobile data

NFC and payment
Make mobile payments, share data, and read or write NFC tags

Location Services

Whenever you take a photo, data on your location is saved inside of the photo's called EXIF data. When you send that photo to someone or post it online, data on where you took the photo may be available to those who know how to view it. If you post a picture that you took from your home, anyone that can view it may be able to figure out where you live and more.



11:24

Settings

Personal

Location
OFF

Security

Accounts

Google

Languages & input
English (United States)

Backup & reset
Back up disabled

To disable your location from being shared, select "Settings" and scroll down to "Biometrics and security." Disable your location services

Google Maps will use your location history and travel times to notify you of traffic before you travel. #GoogleIsWatching

UPDATED JAN 2021

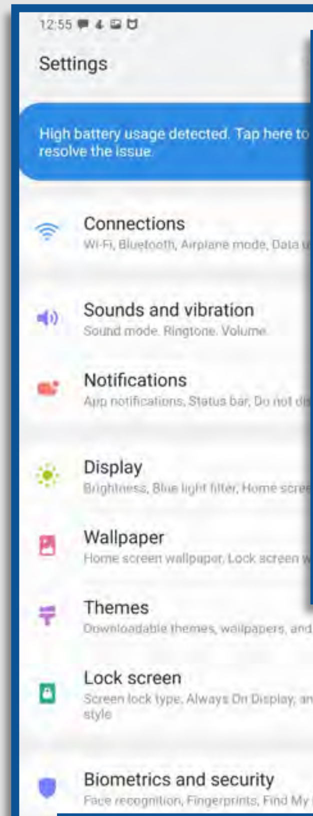
ANDROID PRIVACY SETTINGS (ANDROID 10.0)

Lost/Stolen Phone

Over 100 cell phones are lost or stolen in the U.S. every minute, which shows how necessary it is to keep your device secure and locked with biometrics or a passcode. All Android phones work by synching a phone to a google account, so if you lose your device, you can go to **android.com/find** in order to locate it. This is the native “Find My Device” tool for Android, and is automatically enabled on your Android Smartphone. Alternatively , you can download the “Find My Device” app from Google Play Store.

- Locate Android devices associated with your Google account.
- Reset your device's screen lock PIN.
- Erase all data on the phone.

Note: If you turn off “Location Services” in the “Location Setting” menu, you cannot use “Location Services” for apps that locate lost or stolen devices. You can still wipe your phone if the “Location Services” are “off” . If you wish to use some “Location Services”, be sure to go into each app and set the “Location Settings” as desired rather than turn off the main “Location Services” setting.



12:55

Settings

High battery usage detected. Tap here to resolve the issue.

Connections
Wi-Fi, Bluetooth, Airplane mode, Data u

Sounds and vibration
Sound mode, Ringtone, Volume

Notifications
App notifications, Status bar, Do not di

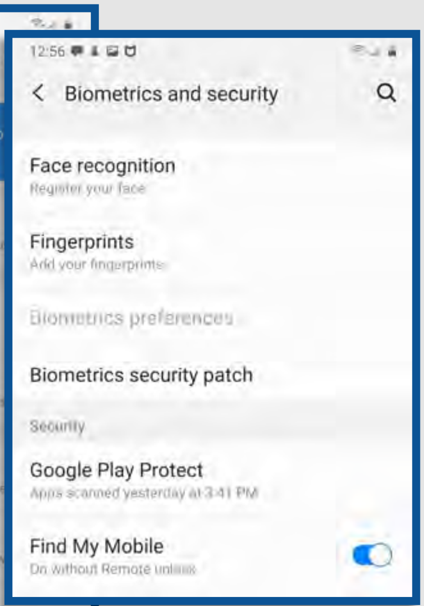
Display
Brightness, Blue light filter, Home scre

Wallpaper
Home screen wallpaper, Lock screen w

Themes
Downloadable themes, wallpapers, and icons

Lock screen
Screen lock type, Always On Display, and Clock style

Biometrics and security
Face recognition, Fingerprints, Find My Mobile



12:56

< Biometrics and security

Face recognition
Register your face

Fingerprints
Add your fingerprints

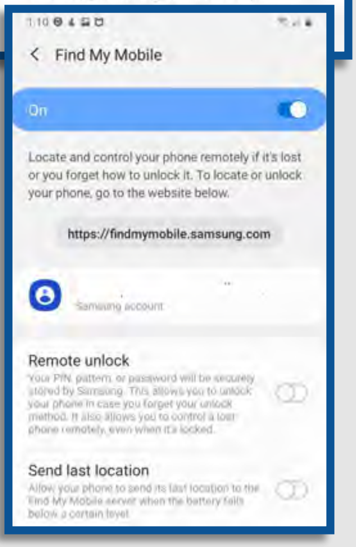
Biometrics preferences

Biometrics security patch

Security

Google Play Protect
Apps scanned yesterday at 3:41 PM

Find My Mobile
On without Remote unlock



1:10

< Find My Mobile

On

Locate and control your phone remotely if it's lost or you forget how to unlock it. To locate or unlock your phone, go to the website below.

https://findmymobile.samsung.com

Samsung account

Remote unlock
Your PIN, pattern, or password will be securely stored by Samsung. This allows you to unlock your phone in case you forget your unlock method. It also allows you to control a lost phone remotely, even when it's locked.

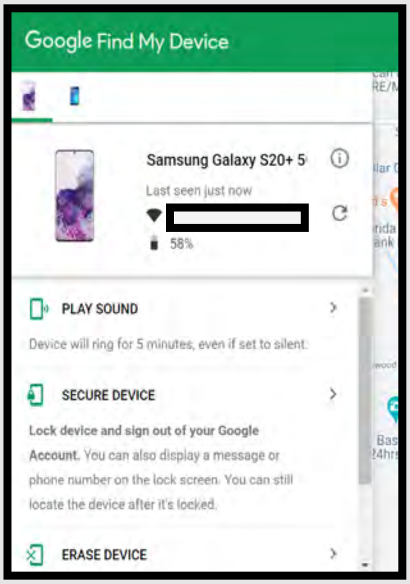
Send last location
Allow your phone to send its last location to the Find My Mobile server when the battery falls below a certain level

What should you do if your device is lost or stolen? Google can help you locate it. Let’s enable the settings on your device so that in case you need to, you can locate your lost phone.

Go into “Settings” > “Biometrics and security” > “Find My Mobile”. Ensure the Toggle is set to “On”

If your device is lost or stolen, you can then go to “Google Find My Device” page and see where your phone was located last. You can make the (**android.com/find**) device ring at full volume to help you find it or remotely lock or erase all data on it.

In order to test this feature, let’s go to **android.com/find** and see if it works.



Google Find My Device

Samsung Galaxy S20+ 5

Last seen just now

[redacted]

58%

PLAY SOUND

Device will ring for 5 minutes, even if set to silent.

SECURE DEVICE

Lock device and sign out of your Google Account. You can also display a message or phone number on the lock screen. You can still locate the device after it's locked.

ERASE DEVICE

Can Android phones get viruses? The traditional “virus” is common on personal computers, Androids don’t get these traditional viruses, but they do get other malware. This malicious software can be designed to secretly control the device or even steal private information.

An example of this Android malware is Triout. Triout was originally founded in 2018, bundled with a legitimate application on the Google Play marketplace. This malware could hide on your Android and record phone calls, save text messages, record videos, take pictures and collect your location. Although this original version was only active from May 2018 to Dec 2018, there are new variations being discovered. In order to help prevent malware from getting onto an Android device it is important to turn off your Wi-Fi, Bluetooth, and sharing capabilities whenever you are not actively using them.

Although saving your passwords is convenient, it poses a huge threat to your security should your device be stolen.

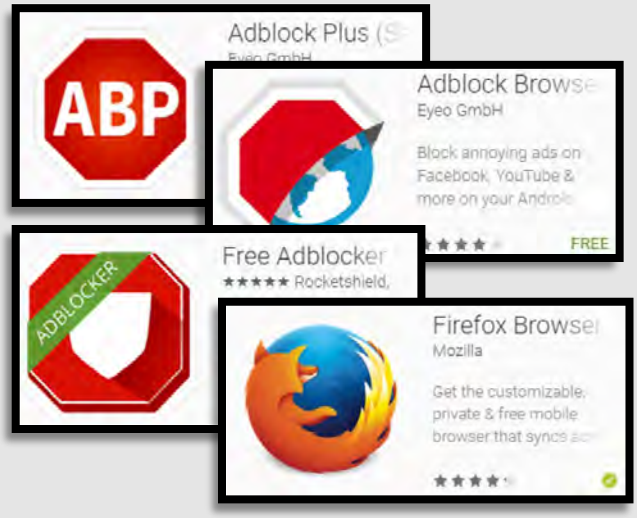
UPDATED JAN 2021

ANDROID PRIVACY SETTINGS (ANDROID 10.0)

Lost or Stolen Android Device

Ad Tracking

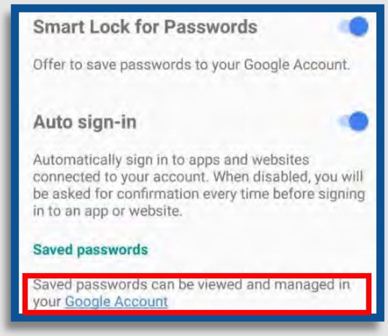
Ads can track everything you do. Not all Android devices and OS versions have settings to turn Ad tracking off. If your device does not have this setting, you can download ad blocking / privacy-oriented browsers or browser add-ons. Here are just a few examples:


Adblock Plus (S
Eyeo GmbH
ABP
Adblock Browse
Eyeo GmbH
Block annoying ads on Facebook, YouTube & more on your Andro
★★★★
FREE
ADBLOCKER
Free Adblocker
★★★★★ Rocketshield,
Firefox Browse
Mozilla
Get the customizable, private & free mobile browser that syncs ac
★★★★

Smart Lock for Passwords

From the same Google Settings section, select "Smart Lock for Passwords". You will then see the screen where you can turn off the options to save your passwords and automatically sign-in to web pages and other account-oriented sites. You can also add apps for which you don't want passwords to be saved.

Alternately, you can select specific accounts and delete the saved password by tapping the "Google Account" hyperlink. All saved passwords are encrypted and stored in the Google cloud storage that comes with your account. Although it is recommended that you turn off the above options, only you can balance your security with the convenience of saved passwords.



Smart Lock for Passwords

Offer to save passwords to your Google Account.

Auto sign-in

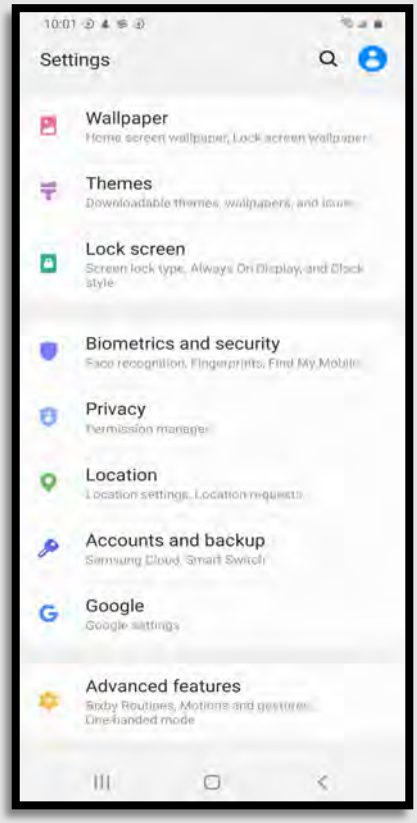
Automatically sign in to apps and websites connected to your account. When disabled, you will be asked for confirmation every time before signing in to an app or website.

Saved passwords

Saved passwords can be viewed and managed in your Google Account

If your device has the option to control advertisements, the following directions show you how to disable the feature:

Go to "Settings" > "Google" > "Ads". Tap the toggle switch to the "On" position for "Opt out of Ads Personalization".



10:01

Settings

Wallpaper
Home screen wallpaper, Lock screen wallpaper

Themes
Downloadable themes, wallpapers, and icons

Lock screen
Screen lock type, Always On Display, and Clock style

Biometrics and security
Face recognition, Fingerprints, Find My Mobile

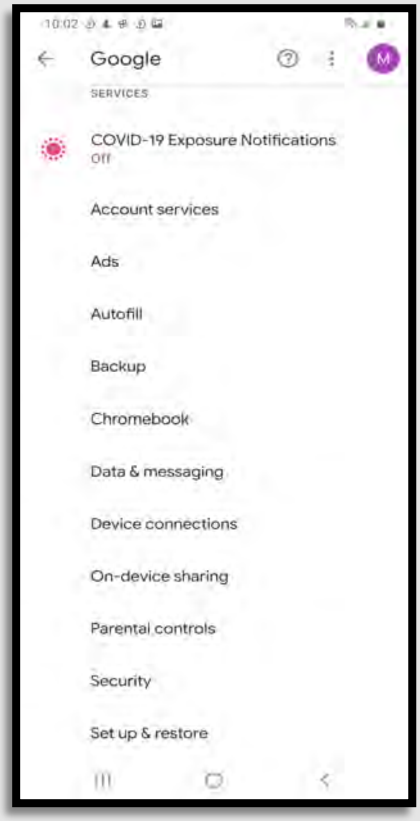
Privacy
Permission manager

Location
Location settings, Location requests

Accounts and backup
Samsung Cloud, Smart Switch

Google
Google settings

Advanced features
Bixby Routines, Motions and gestures, One-handed mode



10:02

Google

SERVICES

COVID-19 Exposure Notifications
Off

Account services

Ads

Autofill

Backup

Chromebook

Data & messaging

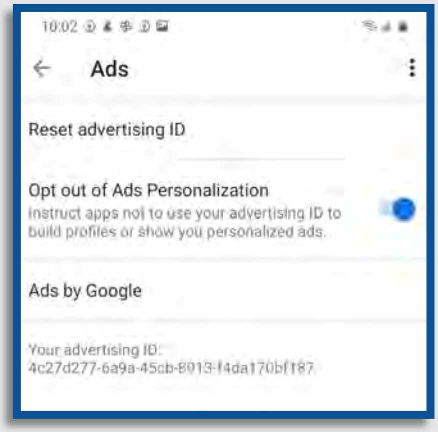
Device connections

On-device sharing

Parental controls

Security

Set up & restore



10:02

Ads

Reset advertising ID

Opt out of Ads Personalization
Instruct apps not to use your advertising ID to build profiles or show you personalized ads.

Ads by Google

Your advertising ID:
4c27d277-6a9a-45cb-8913-f4da170bf187

Safe Browsing: Android devices have a "safe browsing" mode that is built into them and enabled by default. While using Google Chrome, this feature will give warnings before entering a suspicious site. As long as your Chrome and Android are updated to the most recent versions, this feature should work to protect you from malicious sites.

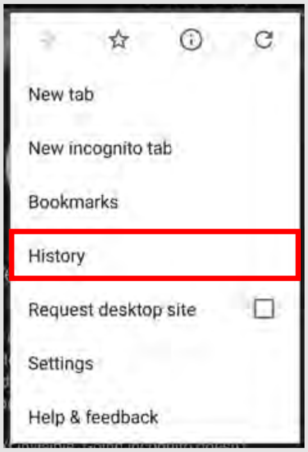
Google Play Protect is Android's native built-in security feature. Ensure that it is on, "Settings" > "Biometrics and security" > "Google Play Protect".

UPDATED JAN 2021

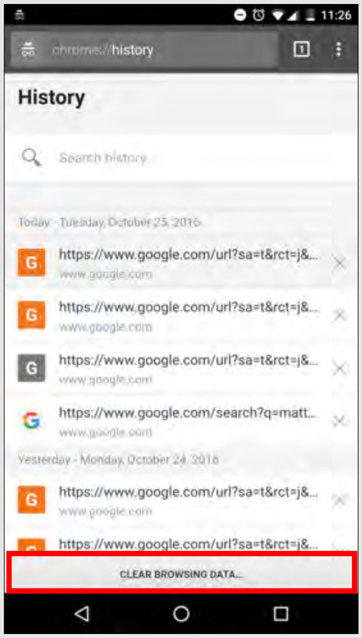
ANDROID PRIVACY SETTINGS (ANDROID 10.0)

Internet Privacy Settings

Browser history and cookies are tracked when browsing the web from your mobile devices. To ensure privacy, open your browser (Chrome) and tap the three dots in the upper right-hand corner. Tap “History” then “Clear Browsing Data” at the bottom (or top) of the screen. On the next screen, select the applicable boxes (use the below screen shot as an example) and tap the blue “Clear Data” button.



New tab
New incognito tab
Bookmarks
History
Request desktop site □
Settings
Help & feedback



chrome://history

History

Search history

Today - Tuesday, October 25, 2016

https://www.google.com/url?sa=t&rct=j&...
www.google.com

https://www.google.com/url?sa=t&rct=j&...
www.google.com

https://www.google.com/url?sa=t&rct=j&...
www.google.com

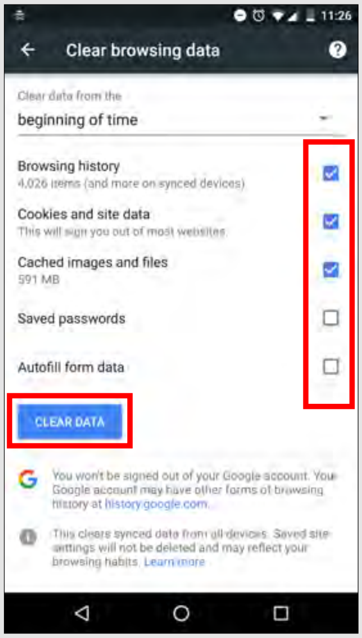
https://www.google.com/search?q=matt...
www.google.com

Yesterday - Monday, October 24, 2016

https://www.google.com/url?sa=t&rct=j&...
www.google.com

https://www.google.com/url?sa=t&rct=j&...

CLEAR BROWSING DATA...



Clear browsing data

Clear data from the
beginning of time

Browsing history ☑
4,026 items (and more on synced devices)

Cookies and site data ☑
This will sign you out of most websites.

Cached images and files ☑
591 MB

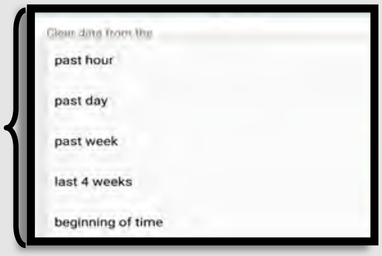
Saved passwords □

Autofill form data □

CLEAR DATA

You won't be signed out of your Google account. Your Google account may have other forms of browsing history at history.google.com.

This clears synced data from all devices. Saved site settings will not be deleted and may reflect your browsing habits. Learn more

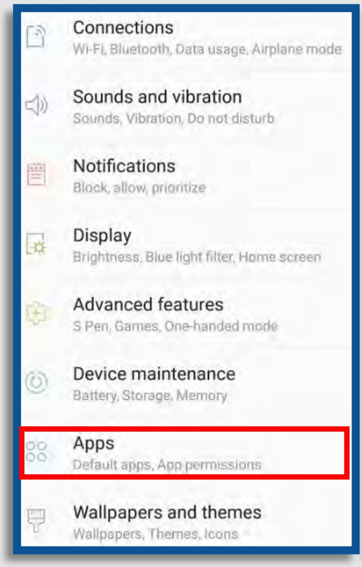


Clear data from the
past hour
past day
past week
last 4 weeks
beginning of time

You have the option here to tap the drop-down arrow and select a date range of data to be deleted. If you get in the habit of clearing your browser history, cookies, and cache then taking this step will become less important.

Application Manager

The applications you load access different capabilities on your device, regardless of whether they are active or working in the background. You can see, and to some degree control, what access each application has in the “Application Manager”.



Connections
Wi-Fi, Bluetooth, Data usage, Airplane mode

Sounds and vibration
Sounds, Vibration, Do not disturb

Notifications
Block, allow, prioritize

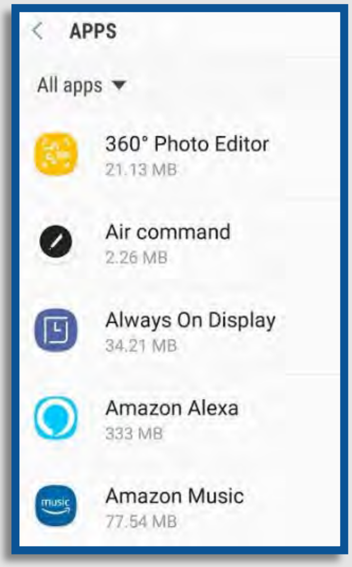
Display
Brightness, Blue light filter, Home screen

Advanced features
S Pen, Games, One-handed mode

Device maintenance
Battery, Storage, Memory

Apps
Default apps, App permissions

Wallpapers and themes
Wallpapers, Themes, Icons



APPS

All apps ▾

360° Photo Editor
21.13 MB

Air command
2.26 MB

Always On Display
34.21 MB

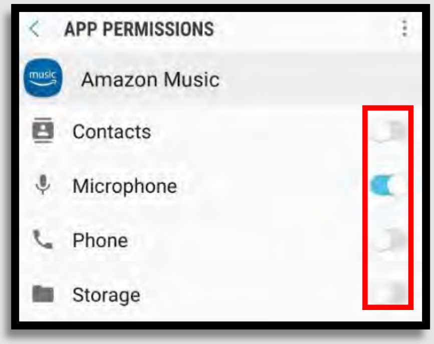
Amazon Alexa
333 MB

Amazon Music
77.54 MB

Go to “Settings” > “Apps” and tap the app you want to view.

Then tap “Permissions”.

This will show you what permissions are granted when you accept the user agreement to download the app. In most instances these permissions can be controlled individually.



APP PERMISSIONS

Amazon Music

Contacts
Microphone
Phone
Storage

This only works with apps designed for use specifically with Android. Permissions for older apps or those without full Android functionality can still be disabled, but this could make the app function unreliably.

Pay attention to user agreements when downloading new apps. Understand what kinds of information the app wants to access from your device.

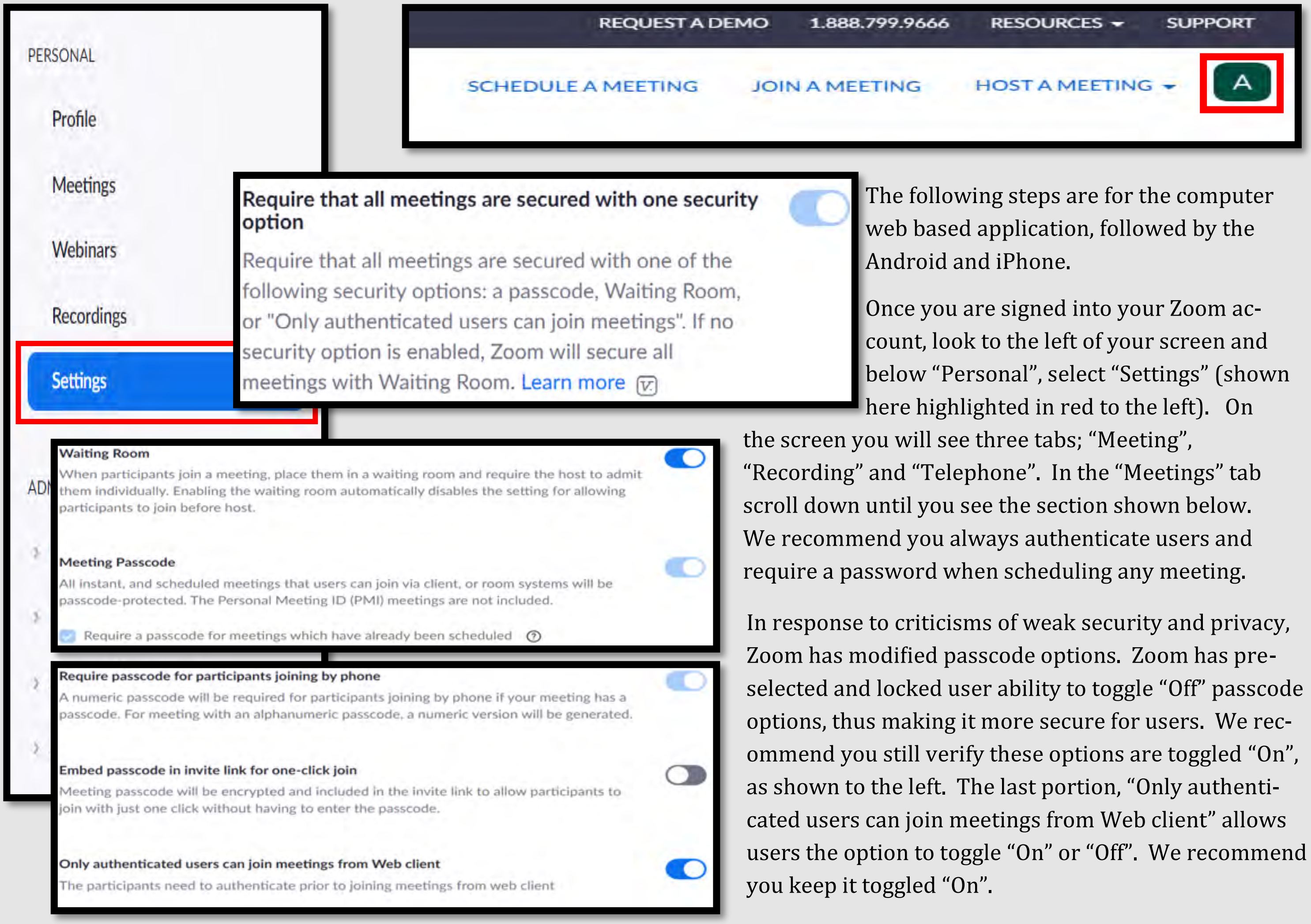
UPDATED JAN 2021

ZOOM SMART CARD

Do's and Don'ts

- ***Do*** require a password for all meetings and webinars conducted in Zoom. This will help to minimize intruders from gaining access to your conferences.
- ***Do*** make sure to control screen sharing capabilities within Zoom. We recommend you never give up control of your personal screen to anyone you are in a meeting with.
- ***Do*** have all attendees register prior to meeting on Zoom in order to dissuade Zoombombers from entering your meetings.
- ***Do*** discuss potential security and privacy concerns with your participants or company prior to using Zoom.
- ***Do*** review updated security notes posted by Zoom.
- Do ***not*** use video call if it is not required. When possible, it is recommended to refrain from using video conferencing in Zoom. Instead, simply dial into meetings, which limits the information you are required to provide.
- Do ***not*** allow participants to share their screen during any of your meetings.
- Do ***not*** forget to lock your meeting once you have confirmed all known participants have entered your meeting domain. Doing so will prevent intruders from gaining access during your meeting.
- Do ***not*** engage a Zoombomber. It is recommended you lock your meeting to prevent intruders.

Zoom is a U.S. based remote conferencing service utilized by businesses, schools and individuals all over the world. It provides a remote conferencing service that combines video conferencing, online meetings, and a messaging feature. Zoom has recently come under scrutiny for its inadequate privacy and security protocols, most notably its lack of encryption and accidental routing of calls through China. While we do not recommend using Zoom for conferencing, the next several pages show recommended ways to manage the security and privacy settings for Zoom, in case you find yourself needing to use it.



Require that all meetings are secured with one security option

Require that all meetings are secured with one of the following security options: a passcode, Waiting Room, or "Only authenticated users can join meetings". If no security option is enabled, Zoom will secure all meetings with Waiting Room. Learn more

Waiting Room

When participants join a meeting, place them in a waiting room and require the host to admit them individually. Enabling the waiting room automatically disables the setting for allowing participants to join before host.

Meeting Passcode

All instant, and scheduled meetings that users can join via client, or room systems will be passcode-protected. The Personal Meeting ID (PMI) meetings are not included.

☑ Require a passcode for meetings which have already been scheduled

Require passcode for participants joining by phone

A numeric passcode will be required for participants joining by phone if your meeting has a passcode. For meeting with an alphanumeric passcode, a numeric version will be generated.

Embed passcode in invite link for one-click join

Meeting passcode will be encrypted and included in the invite link to allow participants to join with just one click without having to enter the passcode.

Only authenticated users can join meetings from Web client

The participants need to authenticate prior to joining meetings from web client

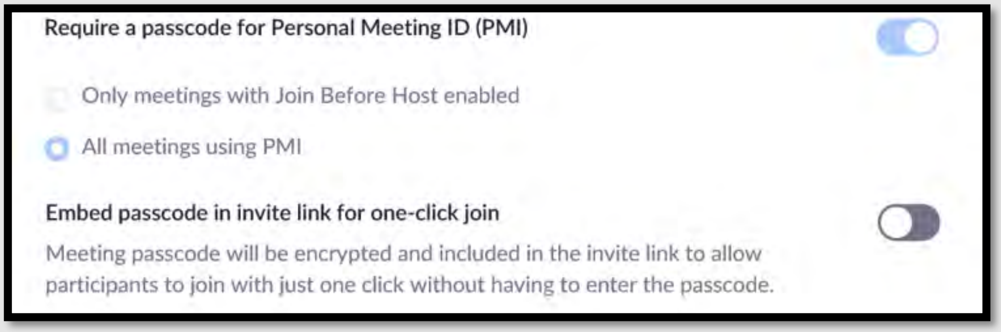
The following steps are for the computer web based application, followed by the Android and iPhone.

Once you are signed into your Zoom account, look to the left of your screen and below "Personal", select "Settings" (shown here highlighted in red to the left). On the screen you will see three tabs; "Meeting", "Recording" and "Telephone". In the "Meetings" tab scroll down until you see the section shown below. We recommend you always authenticate users and require a password when scheduling any meeting.

In response to criticisms of weak security and privacy, Zoom has modified passcode options. Zoom has preselected and locked user ability to toggle "Off" passcode options, thus making it more secure for users. We recommend you still verify these options are toggled "On", as shown to the left. The last portion, "Only authenticated users can join meetings from Web client" allows users the option to toggle "On" or "Off". We recommend you keep it toggled "On".

When using video conferencing it is important to remember to check and secure your network connections. #updateandbesafe.

ZOOM SMART CARD



Require a passcode for Personal Meeting ID (PMI)

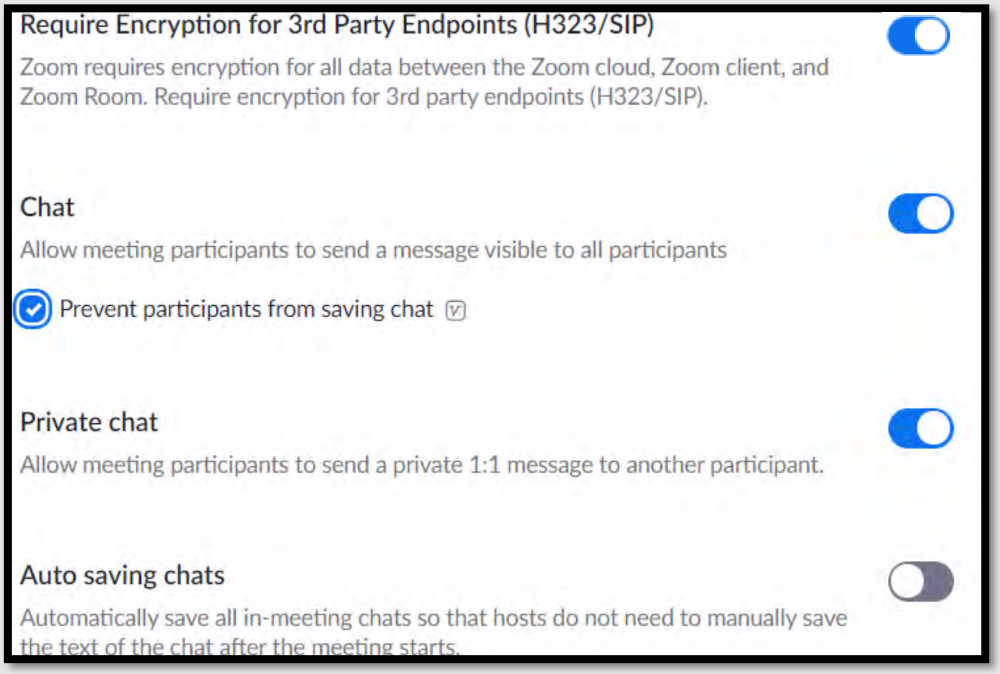
□ Only meetings with Join Before Host enabled

● All meetings using PMI

Embed passcode in invite link for one-click join

Meeting passcode will be encrypted and included in the invite link to allow participants to join with just one click without having to enter the passcode.

To the left you will see a continuation of the password requirements and recommendations located in "Meeting." We recommend you require meeting attendees to input the provided password and ***not*** to embed the password into the meeting link. We also recommend you use a "Pre-meeting Password" and not your "Personal Meeting ID".



Require Encryption for 3rd Party Endpoints (H323/SIP)

Zoom requires encryption for all data between the Zoom cloud, Zoom client, and Zoom Room. Require encryption for 3rd party endpoints (H323/SIP).

Chat

Allow meeting participants to send a message visible to all participants

☑ Prevent participants from saving chat

Private chat

Allow meeting participants to send a private 1:1 message to another participant.

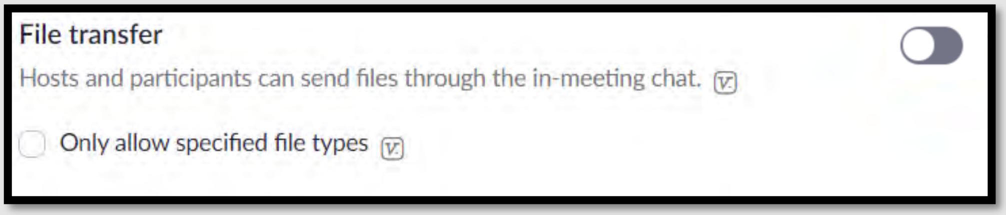
Auto saving chats

Automatically save all in-meeting chats so that hosts do not need to manually save the text of the chat after the meeting starts.

Also, we recommend you use end-to-end encryption whenever possible when using any device that holds your personal information, Zoom is no different.

Note: Zoom's encryption capabilities have been called into question on several occasions. Therefore, we recommend you watch what is documented on Zoom when in a meeting, as the meeting host's encryption may not keep your information secure.

While using chat features on Zoom, we recommend you not allow other attendees to save chats. In order to do this, scroll down until you see "Chat" (shown here to the left). All configurations to the left are recommended for the "Chat" section.

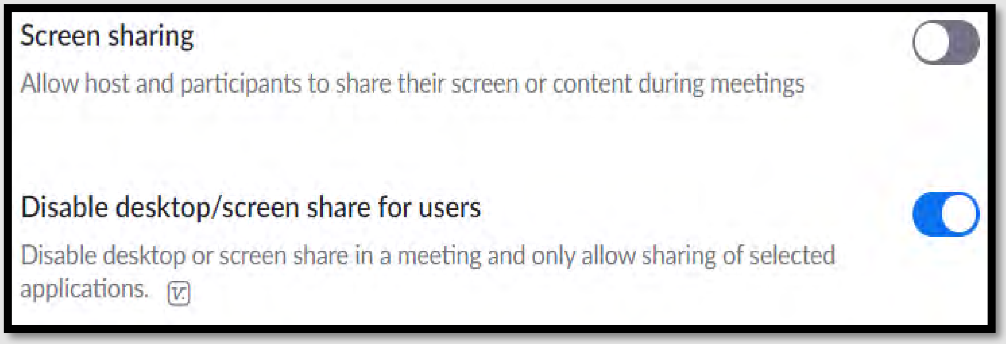


File transfer

Hosts and participants can send files through the in-meeting chat.

□ Only allow specified file types

Scrolling past "Chat" you will find "File transfer" next in your "Meeting" tab. Due to Zoom's lack of acceptable encryption and recent security issues, we recommend you ***not*** send files of any kind on Zoom.



Screen sharing

Allow host and participants to share their screen or content during meetings

Disable desktop/screen share for users

Disable desktop or screen share in a meeting and only allow sharing of selected applications.

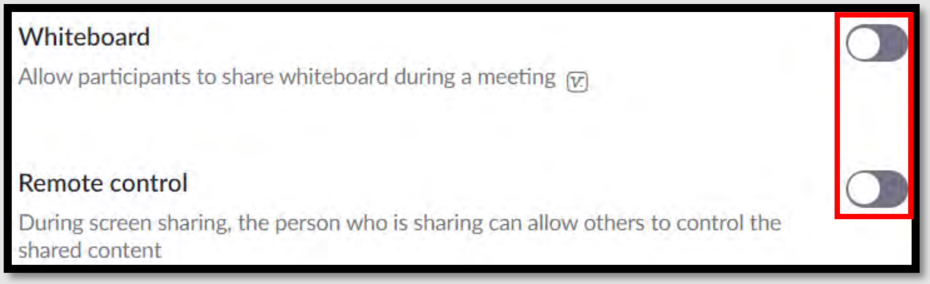
Next, scroll down to "Screen sharing". We recommend you ***not*** allow the ability to screen share when in a meeting on Zoom. If you must allow screen sharing, we recommend that users control who can share screens and who can take control of those screens.

. It is important to think about what people can see and hear when using Zoom. Encourage the use of virtual backgrounds so attendees' personal environments are not shown.

UPDATED JAN 2021

ZOOM SMART CARD

As you continue to scroll down, we recommend you disable the sections "Whiteboard" and "Remote control" (highlighted here in red). It is never recommended that Users give up control of their own computer to any other individual, whether it is a personal computer or company computer.

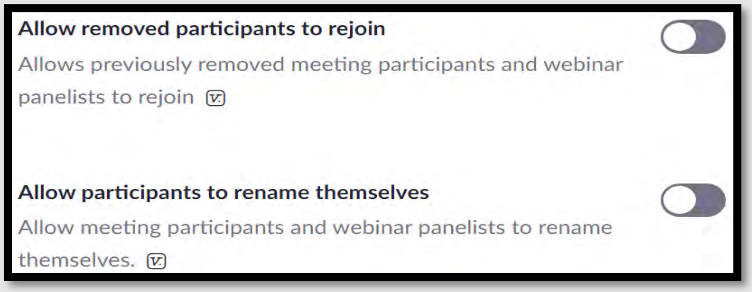


Whiteboard ○

Allow participants to share whiteboard during a meeting

Remote control ○

During screen sharing, the person who is sharing can allow others to control the shared content



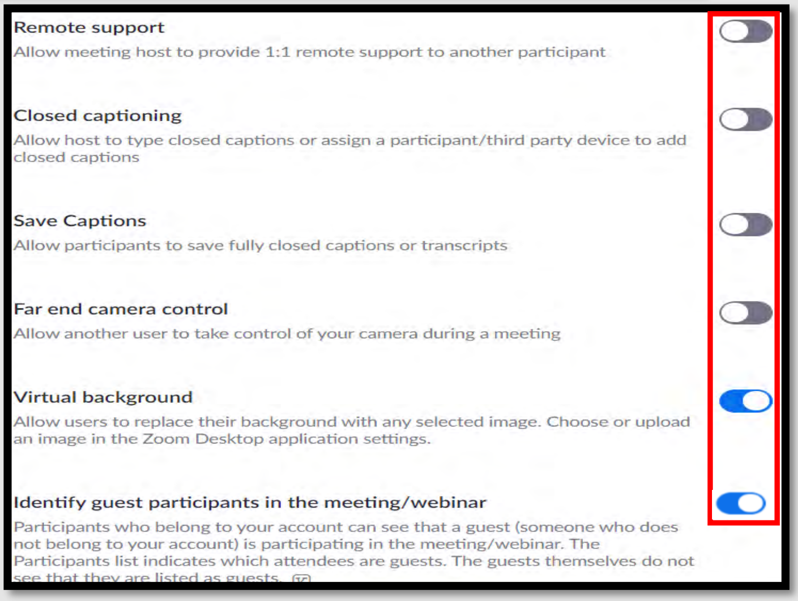
Allow removed participants to rejoin ○

Allows previously removed meeting participants and webinar panelists to rejoin

Allow participants to rename themselves ○

Allow meeting participants and webinar panelists to rename themselves.

New to Zoom is a feature that allows participants to rejoin a meeting if they have been previously removed. It is important you turn this function to "off" in order to prevent users that might hack into your meetings, to continue to rejoin after you have identified and removed them. In order to do so simply scroll down past "Remote Control" and find "Allow removed participants to rejoin" and toggle it to "off". It is also a good idea to not allow individuals to rename themselves in order to prevent any confusion from other participants.



Remote support ○

Allow meeting host to provide 1:1 remote support to another participant

Closed captioning ○

Allow host to type closed captions or assign a participant/third party device to add closed captions

Save Captions ○

Allow participants to save fully closed captions or transcripts

Far end camera control ○

Allow another user to take control of your camera during a meeting

Virtual background ●

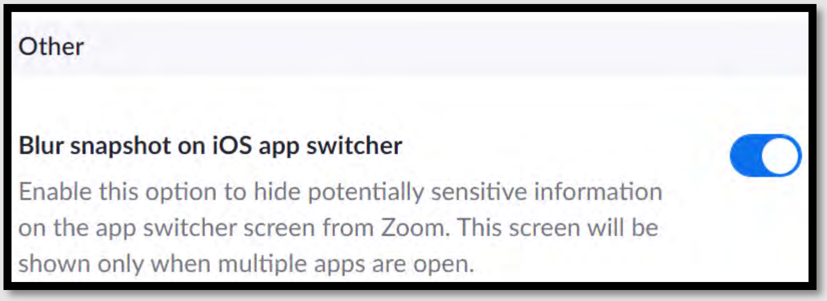
Allow users to replace their background with any selected image. Choose or upload an image in the Zoom Desktop application settings.

Identify guest participants in the meeting/webinar ●

Participants who belong to your account can see that a guest (someone who does not belong to your account) is participating in the meeting/webinar. The Participants list indicates which attendees are guests. The guests themselves do not see that they are listed as guests.

Once you have set the above recommendations, continue to scroll down until you find the "In Meetings (Advanced)" section. Here you will find a series of settings that need to be updated/checked to ensure they meet your specific security requirements. However, we recommend meeting attendees ***not*** participate in any third party activities while on Zoom. We also recommend users ***not*** allow other users to take control of their camera while using Zoom. When setting up a meeting or webinar, it is important to ensure you are able to see "guests" who might be participating for both you and your contacts. If you scroll down, still in "In Meetings (Advanced)," you can enable the "Identify guest participants in the meeting/ webinar" (shown to the left).

If you scroll all the way to the bottom of this section you will find yet another new section on Zoom. This final section will allow you to blur any photos that are being made from users on smart devices in order to control proprietary information or other individuals who might be in attendance. If you are using Zoom for business functions it is important that you enable this function to ensure your companies privacy.



Other

Blur snapshot on iOS app switcher ●

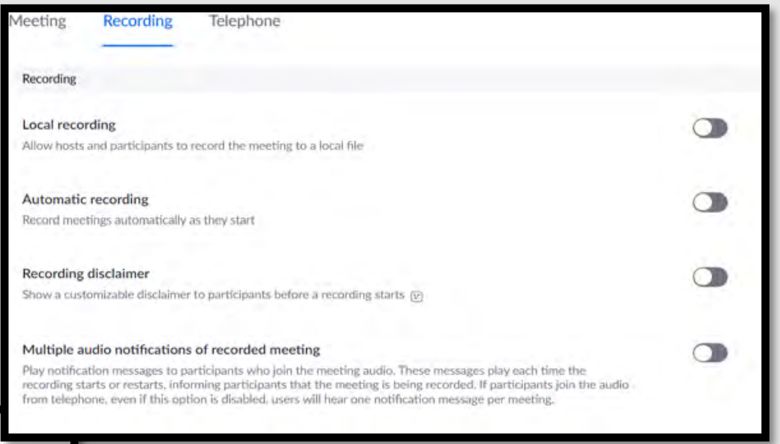
Enable this option to hide potentially sensitive information on the app switcher screen from Zoom. This screen will be shown only when multiple apps are open.

When possible use a Co-Host or an Alternate Host to help monitor activity during your meeting.

UPDATED JAN 2021

ZOOM SMART CARD

Now, scroll back to the very top of the screen and select "Recording" from the menu option (shown to the right, selected in blue). Though there are not very many selections to go through, it is still very important to review all your settings here and enable or disable any features you see fit. We recommend you disable most, and preferably all, features located in the "Recording" section. The only exception here would be the very last feature, which is more of a personal preference than a security issue. We recommend you ***not*** allow anyone to record your meetings.



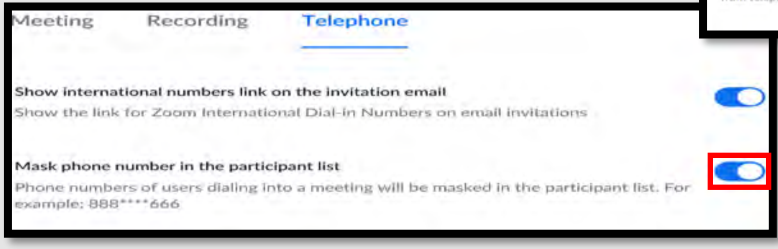
Recording

Local recording
Allow hosts and participants to record the meeting to a local file

Automatic recording
Record meetings automatically as they start

Recording disclaimer
Show a customizable disclaimer to participants before a recording starts

Multiple audio notifications of recorded meeting
Play notification messages to participants who join the meeting audio. These messages play each time the recording starts or restarts, informing participants that the meeting is being recorded. If participants join the audio from telephone, even if this option is disabled, users will hear one notification message per meeting.

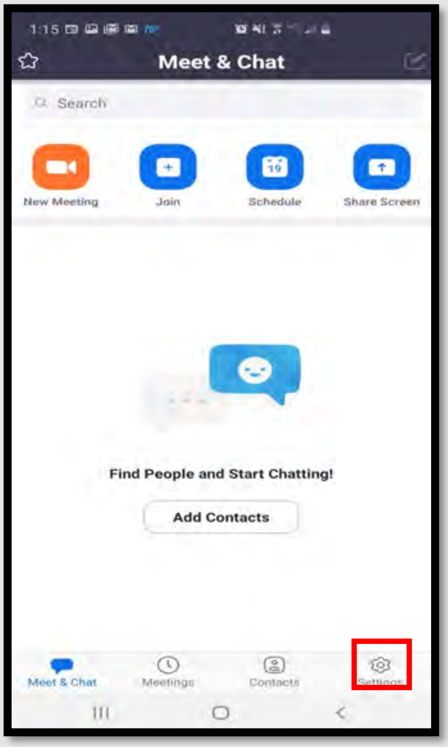


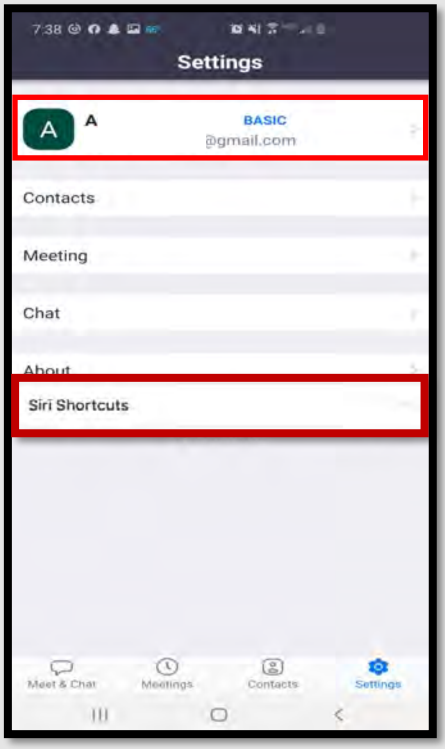
Show international numbers link on the invitation email
Show the link for Zoom International Dial-in Numbers on email invitations

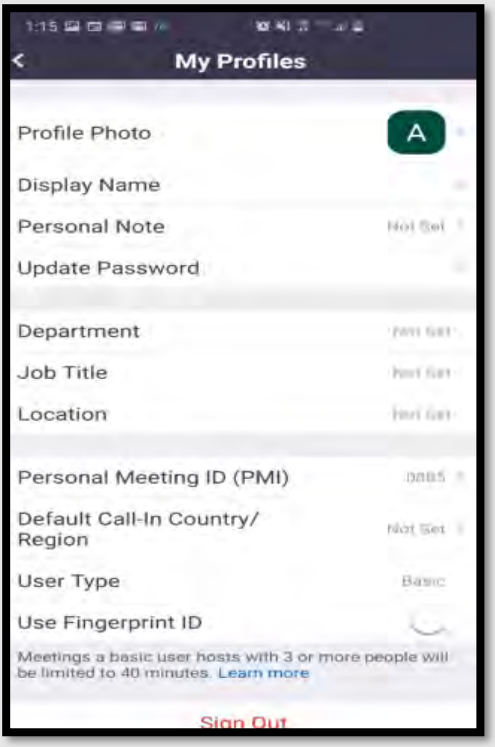
Mask phone number in the participant list
Phone numbers of users dialing into a meeting will be masked in the participant list. For example: 888****666

Head back up to the menu and select "Telephone" to review the final settings here. First, we recommend that you mask meeting attendees' phone numbers. In order to do this, simply toggle the "Mask phone number in the participant list" to enable (shown to the left in red).

When using Zoom on your smartphone there are a few security and privacy settings that should be considered for safe use. Though it is not recommended for use on your smart phone, should you chose, there are a few settings to consider here. On both the Android and iPhone, look to the lower right of your screen and select "Settings" (shown below to the left in red). Next, select your name/email from the top of the screen to take you to your profile page. NOTE: iPhone Users, before selecting your name/email you can look to the lower portion of your screen to "Enable" or (recommended) "Disable" any "Siri Shortcuts" related to this application. In your "My Profiles" section, review each individual section and ensure no personal information has been provided. It is recommended you use initials for your "Display Name," write no "Personal Notes" about yourself and not fill in any other personal information about yourself or the company you are affiliated with unless otherwise directed.







Holding participants in a "waiting room" and approving the connection of each individual gives the host control over who is in the meeting.

UPDATED JAN 2021

ZOOM SMART CARD

Do you think your account may have been compromised or hacked? Have you noticed any of the following:

- Unexpected calls or messages made or received from your account
- Any Direct Messages sent from your account you did not initiate
- Other account behaviors you didn't perform or approve (like following, unfollowing, blocking, etc.)
- A notification from Zoom stating your account may be compromised
- A notification from Zoom stating your account information (bio, name, etc.) has changed
- Your password is no longer working or you are being prompted to reset it. *If this occurs it is highly recommended you sign-in online and change your password immediately

If you said "Yes" to any of the above, it is recommended you immediately do the following actions:

- Delete any unwanted messages that were posted while your account was compromised
- Scan your computers for viruses and malware, especially if unauthorized account behaviors continue to be posted after you've changed your password
- Make sure to change your password. Always use a strong password you haven't used elsewhere and would be difficult to guess
- Consider using login verification (if you haven't done so already), instead of relying on just a password. Login verification introduces a second check to make sure you and only you can access your Zoom account. Note: Two Factor Authentication for Zoom ONLY works on the web based app and only if you are an admin or if the admin has set it up for you.
- Be sure to check your email is secure. It may be worth changing the password to both your Zoom account and the email associated with your Zoom account.

If you need to report a violation of Zoom's Terms of Services follow this link: https://support.zoom.us/hc/en-us/articles/200613919-Report-Terms-Of-Use-Violation

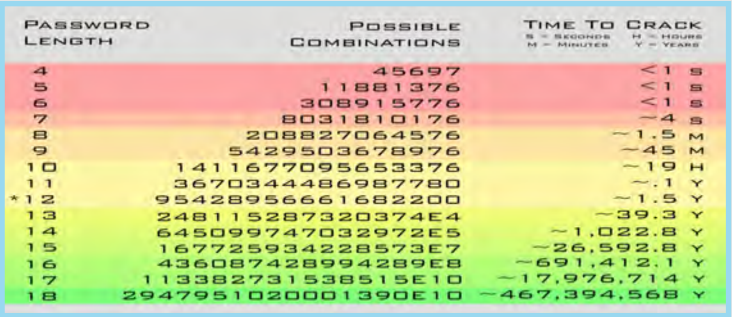
If you would like to terminate your account follow this link: https://zoom.us/account

If you cannot log in to your email account, **Twitter** has provided links to each email account "having trouble signing in" page for your convenience. Please see the **Twitter** smart card for this information.

If you still need help or have questions, you can always contact

Zoom using their Support site at: https://support.zoom.us/hc/en-us/articles/201362003

THERE IS NO TRY, THERE IS ONLY DO...
If you want to protect your passwords from the Dark Side.



Password Length	Possible Combinations	Time To Crack
		S = Seconds H = Hours
		M = Minutes Y = Years

4	45697	<1 S
5	11881376	<1 S
6	308915776	<1 S
7	8031810176	~4 S
8	208827064576	~1.5 M
9	5429503678976	~45 M
10	141167095653376	~19 H
11	3670344486987780	~.1 Y
*12	95428956661682200	~1.5 Y
13	2481152873203 74E4	~39.3 Y
14	6450997470329 72E5	~1,022.8 Y
15	1677259342285 73E7	~26,592.8 Y
16	4360874289942 89E8	~691,412.1 Y
17	1133827315385 15E10	~17,976,714 Y
18	2947951020001 390E10	~467,394,568 Y

Important Information Regarding Zoom: If your Zoom meeting gets "Zoombombed" there are a few things that can be done. First you can lock them out by going to the "Participants List" in the navigation bar and select "more." Next click "Lock Meeting" to prevent any additional intruders from entering your meeting, which will also allow you to remove individuals without them being able to regain access.

If you are less worried about the intruder and more worried about the disruption follow the same path but to the "Participants List" and scroll down to select "Mute All Controls." This option is not recommended for privacy and security concerns.

UPDATED JAN 2021

TRAVELING SAFELY WITH SMARTPHONES

Do's and Don'ts

- ***Do*** enable password and fingerprint locks on your device. Also, protect "Settings" changes on your phone by requiring a password.
- ***Do*** assume that all information on your device can be accessed remotely. Don't store passwords and sensitive information on your phone
- ***Do*** always use complex passwords, the stronger and longer the password the more difficult it will be for someone to hack into.
- ***Do*** delete emails that are old or no longer needed prior to travel. Remember emails contain a lot of personal information. Think about what a hacker might gain if they were able to access your email?
- ***Don't*** become stagnant upon returning from your travels. Examine your smartphone as soon as you return to your home. If it is acting up or repeatedly making you put your password in there may be malware on your device and you may want to take it in or consider getting a new device.
- ***Don't*** link apps and social media accounts together (i.e. using one SM account to login to another). Remember if someone hacks into one of your accounts, it is better if they only get access to that one. Linking accounts together makes all of them vulnerable.
- ***Don't*** leave GPS, Bluetooth, and Wi-Fi turned on when traveling. Any of these left on could allow a hacker to connect to your phone if they were able to get within a certain distance from you.

Wi-Fi Safety Tip

Avoid Public Wi-Fi at all costs, hackers will name the network the same thing as the hotel or other public network. Hackers in Europe have been caught making Public Wi-Fi networks to resemble the public network name. Do not assume all networks are secure, just because it says the name of a company does not mean it is a legitimate network, check with the company to be sure. Also, be sure to turn your Wi-Fi off when you are not using it in order to prevent tracking or hacking of your phone.

Precautionary Tips

- Be aware that your phone may be scanned forensically when entering a foreign country.
- Set your phone to lock automatically and make sure you have a complex password or fingerprint enabled while traveling. This will help to limit an intruders ability to break into your phone if you happen to misplace it.
- Consider installing a VPN to ensure more secure online activity.
- Turn off Wi-Fi and Bluetooth when traveling. Only turn these capabilities on when absolutely necessary, then turn them off when done.
- Purchase SIM Cards for international travel in the U.S. prior to departure. This will ensure not only your security but functionality with your device. If you do decide to use a SIM card make sure to turn off "Auto Sync" to conserve your battery and data plan.
- Make sure all the software is updated on your phone, this will in turn ensure the most up to date security patches are installed on your device.
- Make sure to backup all your data before traveling, so that if your phone or data is lost you can easily restore the information and won't be without important contacts and travel information.
- When feasible, recommend purchasing a pay-as-you-go phone for travel, especially travel overseas. This is probably the single best way to prevent any of your personal information from getting into the wrong hands should you lose the phone.
- Make sure to use your own charger and cables, try not to purchase them from your destination.

Traveling internationally can present new problems, ensure you prepare yourself ***before*** you travel not once you are there.

UPDATED JAN 2021

IDENTITY THEFT SMART CARD

Identity Theft Scams On The Rise

Utility Bill Scam: As of September 2018, the Federal Trade Commission (FTC) reported an increase in local utility scams. The consumer receives a call from someone posing as a local utility company claiming the consumer has a past due bill. The caller is very convincing, even to a consumer who may have just paid their bill. Oftentimes the caller will threaten to cut off service, hoping this threat is enough to get the consumer to provide personal and financial information, thereby falling for the scam. If you feel a call from someone claiming to be a bill collector is suspicious in any way do NOT settle the bill at that time. You have the right to call the utility company yourself but remember do not use the phone number they provided you, look up the number yourself. Also, report this suspicious activity to the FTC.

"Do you know what an overdue bill could do to you credit?"

Imposter Scams: Reports of IRS impostors have surfaced during the 2018 tax season. Consumers receive a call from an individual claiming to be an "IRS Officer," who will then inform the consumer that they owe a large amount of money and if they don't pay an agreed upon amount immediately local law enforcement will issue a warrant for their arrest. They will often try to "negotiate" a smaller amount to make the consumer feel as if they are getting a deal. Instead of paying with a check or money order, these scammers instruct their victims to buy gift cards and read the numbers to the fake agent over the phone for verification. Remember, no legitimate organization will ever ask for payment in gift cards! Also, report all scams involving taxes or the IRS to the IRS fraud department.

"Just pay with Amazon gift cards or I will send the police to your house tonight!"

"Your Social Security Number was just used in a crime, we can help you"

Suspended Social Security Number: Consumers are reporting a new "government related scam." The consumer receives a call and is told that their SSN was used in criminal activity. The caller will claim that the SSN has been suspended and they can help the victim get the situation cleared up. The Social Security Administration does NOT suspend SSNs, ever! Do not give personal information out to callers. If you feel you've been scammed, report it to the FTC immediately. Also, personally look up the number of and call the agency the scammer(s) claim to represent. Make a detailed record of the interaction and be prepared to provide as much information as possible.

Mobile Phone Scams: This scam was identified when a consumer received an email from their mobile phone provider. The email stated, "Your new mobile phone is on its way" and listed a delivery address that didn't belong to the consumer, it was actually the address of a local hotel. Further investigation revealed that someone had used a fake identity to obtain the consumers account information and ordered the additional phone on the consumer's account.

Report fraud & identity theft scams to the FTC at 1-877-FTC-HELP (1-877-382-4357) or online: ftc.gov/complaint

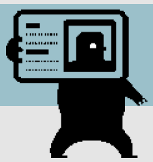
12 Practices to Avoid Identity Theft

1. Do not disclose your full nine-digit Social Security number
2. Avoid paper billing by requesting secure electronic statements instead, or have them mailed to a Commercial Mail Receiving Agency (CMRA)
3. Lock your mailbox
4. Keep your information safe, both online and offline, by shredding documents containing personal information and passwords and protecting sensitive computer files
5. Use unique, hard-to-guess passwords that include a combination of letters, numbers, and symbols
6. Avoid using the same password across multiple accounts
7. Install and update antivirus, anti-malware, and security programs on all computers, tablets, smartphones and operating systems
8. Don't disclose information commonly used to verify your identity on social network sites such as; date of birth, city of birth, mother's maiden name, and name of high school
9. Avoid making purchases, paying bills, or sending sensitive information over unsecured WiFi networks
10. Disable Bluetooth on devices when not in use
11. Watch out for "phishing" scams; do not trust unsolicited offers and ads
12. Fight "skimmers" by touching ATMs to see if all the parts are solid and not add-ons, cover the keypad/screen with your hand while typing the password, and always look for suspicious holes or cameras

Phone Scammers will say anything to get you to disclose personal information; always offer to call back on your own

UPDATED JAN 2021

IDENTITY THEFT SMART CARD



Preventing Other IRS Scams and Fraud

It is very common for criminals to file IRS Tax returns using stolen identities. The fraudsters will typically file early and claim their tax refunds before the victim is aware. It is only when the victim attempts to file their own, valid tax forms that they are informed a refund has already been issued. Victims of identity theft can request a PIN to prove their identity when they file their tax return.

According to the FTC, identity theft was the top complaint received for the past 15 years, increasing 47% from 2014 to 2015 as a result of a massive rise in tax-related identity theft (see "FTC Releases Annual Summary of Consumer Complaints," March 1, 2016).

Children also Victims of Tax Fraud and Identity Theft

Increasingly children are becoming victims of identity theft and tax fraud. Criminals will obtain Social Security numbers or will attempt to obtain credit cards in the names of minor children. It is only when parents attempt to obtain legitimate cards for their children that they discover their children have been targeted. To prevent this, parents may place freezes on accounts for their children to ensure no new credit is issued until they are ready.

What to Do if Your Identity is Stolen

The FTC has put together a great, step-by-step guide on what to do if you think your identity has been stolen (link below). Here’s where to start: https://www.identitytheft.gov/steps

Take action immediately! Keep records of your conversations and all correspondence.

Flag Your Credit Reports. Contact the fraud department of the three major credit reporting agencies. Tell them you are an identity theft victim. Ask them to place a "fraud" alert in your file. An initial fraud alert is good for 90 days.

♦ Equifax 1-800-525-6285

♦ Experian 1-888-397-3742

♦ TransUnion 1-800-680-7289

Order Your Credit Reports. Each company’s credit report about you is slightly different, so order a report from each company. They must give you a free copy of your report if it is inaccurate because of fraud. When you order, you must answer some questions to prove your identity. Read your reports carefully to see if the information is correct. If you see mistakes or signs of fraud, contact your creditors about any accounts that have been changed or opened fraudulently. Ask to speak with someone in the security or fraud department.

Create an Identity Theft Report and Report it to the Local Police. An Identity Theft Report can help you have fraudulent information removed from your credit report, stop a company from collecting debts caused by identity theft, and get information about accounts a thief opened in your name.

To create an Identity Theft Report:

♦ File a complaint with the FTC at ftc.gov/complaint or 1-877-438-4338; TTY: 1-866-653-4261. Your completed complaint is called an FTC Affidavit.

♦ Take your FTC Affidavit to your local police, or to the police where the theft occurred, and file a police report. Get a copy of the police report.

For more information regarding identity theft, visit the following websites:

Federal Trade Commission (FTC) **http://www.consumer.ftc.gov/features/feature-0014-identity-theft**
FTC Identity Theft Online Complaint Form **https://www.ftccomplaintassistant.gov/**
www.fraud.org (You can also call: 1-800-876-7060)

You can get free copies of your credit report once a year from each agency, get one every four months to monitor your credit

UPDATED JAN 2021

KEEPING YOUR CHILDREN SAFE ONLINE

- An April 2015 Pew Research Center study revealed that 92% of teens report going online daily – including 24% who say they go online "almost constantly." Most of the teens also have used or use a smartphone. A separate study showed that nearly 40% of 3–4 year olds and two thirds of 5-7 year olds go online.
- Cyber-bullying, malware, and predators are a few dangers that make the Internet an unsafe environment for unsuspecting children. In 2012, the FBI launched Safe Online Surfing (SOS), a challenging but fun and informative game that educates children about online safety. See more at **https://www.fbi.gov/fbi-kids**
- In half of all sex crimes against a minor involving a social networking site, the social networking site was used to initiate the relationship. 55% of teens have given out personal information to someone they don't' know, including photos and physical descriptions. **https://www.guardchild.com/social-media-statistics-2/**
- 67% of teenagers say they know how to hide what they do online from their parents. 43% of teens say they would change their online behavior if they knew that their parents were watching them.

Do's and Don'ts

- ***Do*** only connect with gamers and online profiles of people you know and trust. Review connections often.
- ***Do*** assume ALL information and images you share are publicly viewable, regardless of your settings.
- ***Do*** use a picture of something other than yourself for your profile photo. Profile photos are viewable to the public.
- ***Do*** tell kids to let parents or responsible adults know anything online makes them uncomfortable.
- Do ***not*** use location services.
- Do ***not*** add your birthdate, location, phone number, or other personal details to online profiles.
- Do ***not*** forget your children have online privacy rights as well. If you are unsure what those rights or laws are you can find them here: **https://www.ftc.gov/consumer-protection/childrens-privacy**

YouTube

Now it is time to give this app another look. YouTube Kids has just pushed their parent-approved content, a control that lets you select every video and channel available to your child. It is available today on Android and coming soon to iOS. In the "Restricted mode", kids are not able to search for content on their own.

Open settings and scroll down to the bottom just past your child's (or your) profile. Select "approved content only" or "Restricted Mode On." Next, you may want to also Lock "Restricted Mode" on this browser. "Restricted Mode" lock prevents others from changing the "Restricted Mode" settings on this browser.

https://www.youtube.com/yt/kids/

CONTROL WHAT APPLICATIONS GET INSTALLED ON YOUR CHILD'S DEVICE

One of the best ways to help protect your child online is to monitor what applications they are using. For iOS users it is recommended that parents keep the Apple ID password and not provide it to the child using the device. Also, make sure that the iPhone requires the password before any downloads can take place. This can also be done on your Android devices as well.

Extras to Help Parents:

Can you set age restrictions on Disney +? The answer is no. You can learn more about this topic here: https://www.androidauthority.com/disney-plus-parental-controls-1108634/

Setting up router controls for your kids: https://kb.netgear.com/25687/How-do-I-set-up-Live-Parental-Controls-on-my-NETGEAR-router-using-the-genie-desktop-app

Your child's "right to privacy" doesn't supersede your right to protect them. Their smartphone is yours for the monitoring, after all who gets the bill? #keepourkidssafeonline

UPDATED JAN 2021

KEEPING YOUR CHILDREN SAFE ONLINE

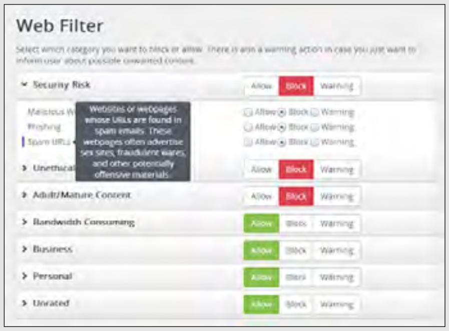
Google has it's own Safety Center to help ensure your kids remain safe Online, stay up to date at www.google.com/safetycenter/families/start/ #themoreyouknow

Security Applications

A variety of paid software packages are available for monitoring your child's online activities. The following packages are effective tools for monitoring or preventing access to certain online content.

Blocksi Web Filter

Blocksi Web Filter is a web filter and parental control extension for Google Chrome. It can be configured to protect your family from inappropriate content on the Internet.



Web Filter

Select which category you want to block or allow. There is also a warning action in case you just want to inform user about possible unwanted content.

- Security Risk: Allow | **Block** | Warning
  - Malicious W…: ○ Allow ● Block ○ Warning
  - Phishing: ○ Allow ● Block ○ Warning
  - Spam URLs: ○ Allow ● Block ○ Warning
- Unethical…: Allow | **Block** | Warning
- Adult/Mature Content: Allow | **Block** | Warning
- Bandwidth Consuming: **Allow** | Block | Warning
- Business: **Allow** | Block | Warning
- Personal: **Allow** | Block | Warning
- Unrated: **Allow** | Block | Warning

Websites or webpages whose URLs are found in spam emails. These webpages often advertise sex sites, fraudulent wares, and other potentially offensive materials.

Net Nanny®

Net Nanny Social lets you keep track of all your children on social media including Facebook, Twitter, Google+, Instagram, Pinterest, and LinkedIn. Features include:

- Detects registered accounts any new accounts created
- Ability to identify cyberbullying, cyber-stalking, or grooming
- Access to view photos and videos child has published
- Alert Notifications
- Daily/Weekly Reports

My Mobile Watchdog

Monitor your child's cell phone use, including call logs, texting, photos (MMS), web history, web filtering, time restrictions, sync contacts and block applications. Receive real time alerts when a stranger contacts your child. Must be installed on your child's phone.

- Monitor your child's cell phone use
- Includes Web filtering, time restrictions, app blocking, and more
- Get real time alerts when a stranger calls the child's phone
- Location Tracking! Track up to 99 locations and know exactly where your child is at any time.
- DailyWatch Summaries! A daily breakdown of your child's activity conveniently packaged and sent to your email.

Microsoft Family Safety

Microsoft family is a free service that helps families stay connected, and keep kids safer on Windows 10 and Xbox One devices, along with Android devices running Microsoft Launcher. You'll find settings like activity reporting, screen time limits, location sharing, and content restrictions on account.microsoft.com/family, where you can also track kids' spending and add money to their Microsoft accounts.

Qustodio

Free parental control app that offers simple tools to manage kids' screen time, filter content and monitor or block apps kids use. Premium features include:

- SMS Messages & Call Tracking
- Location Tracking & Panic Button
- Ability to view social media activity including Facebook, Twitter, Instagram, and Whatsapp
- Block pornography
- Set multi-device time limits
- Control games and apps
- Browser-independent content filter that handles HTTPS traffic

Norton by Symantec Family Premier

Includes support across Windows, Android and iOS devices (no MAC support):

- Web supervision that allows warnings, blocking, or monitoring of sites based on your own site category choices
- Video tracking
- Control SMS contacts on Android
- Email Alerts
- Online time limits
- Activity Tracker to view device Internet history
- Location tracking to know where your child is at any time

UPDATED JAN 2021

PHOTO SHARING SERVICES CARD

Everything we post on the web creates a digital footprint. Protect yourself and your family by carefully choosing what you post.

Do's and Don't's:

- Do share photos only with known and trustworthy people.
- Do use caution when posting images and videos of you or your family. Be aware of your surroundings, to include identifiable locations and any other personal security vulnerabilities.
- Do ensure that family members take similar precautions with their accounts. Their privacy and share settings can expose personal data.

- Don't tag geolocations. The information in these tags can disclose location of where the photo was taken.
- Don't give apps permissions to access the cellphone location services.
- Don't post photos of others, especially children, without getting permission beforehand.

Choosing the right photo sharing service will depend on intent and audience. Key questions to ask:

- ♦ Are you sharing photos primarily for yourself, your friends and family, or for public consumption?
- ♦ Are your contacts and viewers already using a specific service?
- ♦ How much control and privacy do you want over your images? Is the retention of EXIF data problematic?

Although photo sharing services allow you to remove images, not all of them allow you to delete your account. Deleting content and/or account does not ensure removal from the internet or the service provider's systems. Those with access to the photos on a photo sharing service can acquire and redistribute photos as they please. You can find more detailed information on how to set privacy settings for these Services on the following pages.

6 Popular Photo Sharing Services

Service	Primary Use	Image Privacy Options	Retains EXIF	Geo-Location Options (non-EXIF)	Allows Reposting	Populates in Google Searches (Indexed)
Instagram	Share photos and videos from camera enabled mobile devices	**Public;** Private (other users must request to follow you);	No	GPS-based device location and customizable location (both removable)	Yes, only with third party applications	Profiles are indexed, but not photos
snapchat	Share photos and videos that "disappear" after a certain number of views or a period of 24 hours.	**Public;** Private (other users must request to follow you)	No	Snapchat Geofilters use location services on your mobile device. Using Geofilters is optional.	No. Please note that viewers can still screenshot your Snaps.	No
facebook	Social network	**Public;** Only Me; Friends; Friends of Friends	No	Free-form text; location suggestions; map-based (removable)	Yes	Public profiles are indexed
Google Photos	Photo and video sharing and storage service	**Private**; Shared Albums allow anyone with the unique web link to view your photos	Yes	GPS-based from camera and Google's Estimated Location (both can be disabled in the phone settings)	Yes, photos can be downloaded from a Shared Album.	Shared photos may possibly be open to public search in the future
flickr	Photo and video hosting site used for sharing and embedding on blogs and social media	**Public;** Only You, Your Friends, Your Family	**Yes for original uploaded file (not for resized file)**; You can also hide EXIF data	Editable location; map-based (both removable)	Yes	Public albums are indexed; Offers opt-out for 3rd party searches
photobucket	Photo and video hosting site used for sharing and embedding on blogs and social media	**Public;** Private (optional password protection)	Yes for original uploaded file (not for resized file)	Location data is available unless you disable it	**Yes;** No	Public albums are indexed

*Default settings are in **bold**.
**Converting a photo to PNG file format will remove EXIF data.

UPDATED JAN 2021

PHOTO SHARING SERVICES CARD

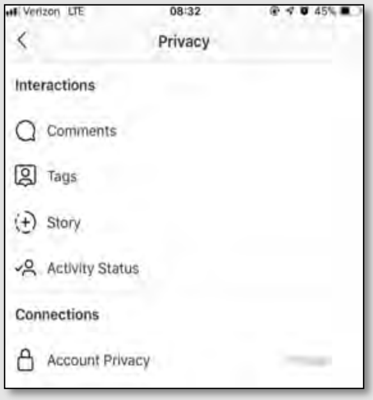
EXIF Removal Tools

- **EXIF Wizard**: https://itunes.apple.com/us/app/exif-wizard/id387652357?mt=8
- **TrashEXIF**: https://itunes.apple.com/us/app/trashexif-metadata-photo-remover/id585543219?mt=8
- **ACDSee Photo Software**: http://www.acdsee.com/
- **Paint Shop Pro Photo Software:** http://www.paintshoppro.com/en/

For more information, please see the EXIF Data Smartcard

Privacy Settings

Instagram



Verizon LTE 08:32 45%

Privacy

Interactions

- Comments
- Tags
- Story
- Activity Status

Connections

- Account Privacy

Tap 👤 on the bottom right.

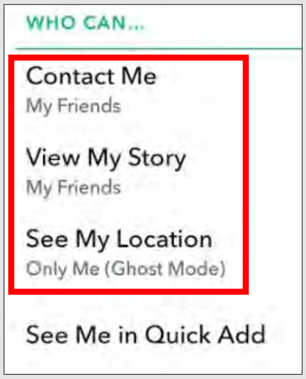
Then tap the menu icon at the top right ≡

Tap ⚙ at the bottom of the screen.

Scroll to find "Privacy" and then ""Account Privacy," make sure the toggle is on for "Private Account".

When your account is private, only people you approve can see your photos and videos.

snapchat



WHO CAN...

Contact Me
My Friends

View My Story
My Friends

See My Location
Only Me (Ghost Mode)

See Me in Quick Add

Tap 👤 at the top.

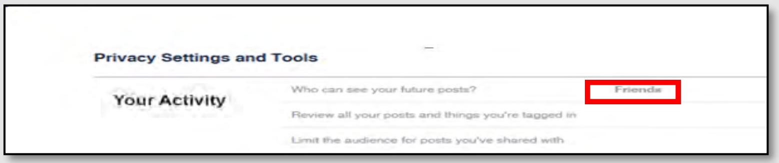
Tap ⚙ to access Settings.

iPhone users, scroll down to the "Additional Services" section. Android users scroll to "Who Can…"

Set each category except "See My Location" to "My Friends".

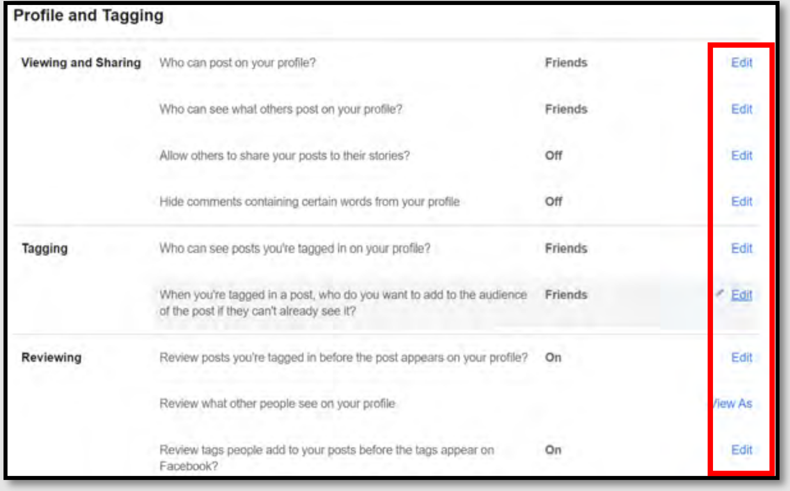
Set "See My location" to "Only Me (Ghost Mode)".

facebook



Privacy Settings and Tools

Your Activity	Who can see your future posts?	Friends
	Review all your posts and things you're tagged in	
	Limit the audience for posts you've shared with	



Profile and Tagging

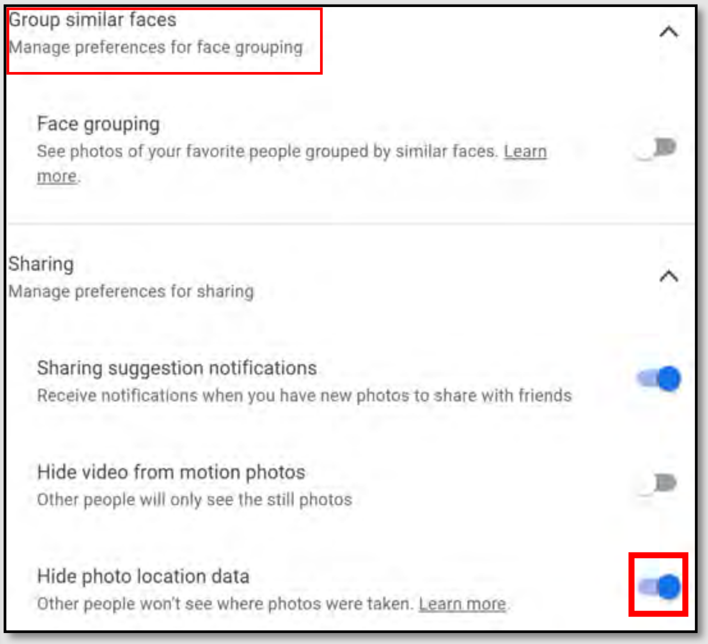
Viewing and Sharing	Who can post on your profile?	Friends	Edit
	Who can see what others post on your profile?	Friends	Edit
	Allow others to share your posts to their stories?	Off	Edit
	Hide comments containing certain words from your profile	Off	Edit
Tagging	Who can see posts you're tagged in on your profile?	Friends	Edit
	When you're tagged in a post, who do you want to add to the audience of the post if they can't already see it?	Friends	Edit
Reviewing	Review posts you're tagged in before the post appears on your profile?	On	Edit
	Review what other people see on your profile		View As
	Review tags people add to your posts before the tags appear on Facebook?	On	Edit

From your smart phone, tap the at ≡ the top right corner.

Select "Settings & Privacy" then "Settings".

Navigate to "Privacy" then to "Privacy Settings" and "Profile and Tagging" to adjust who can see your posts and pictures.

Google Photos



Group similar faces
Manage preferences for face grouping

Face grouping
See photos of your favorite people grouped by similar faces. Learn more. — Off

Sharing
Manage preferences for sharing

Sharing suggestion notifications
Receive notifications when you have new photos to share with friends — On

Hide video from motion photos
Other people will only see the still photos — Off

Hide photo location data
Other people won't see where photos were taken. Learn more — On

At the top of the page select ⚙ to select "Settings".

Under "Sharing," ensure that the toggle is *on* for "Hide photo location data." Ensure that the toggle switch is *off* for "Group similar faces".

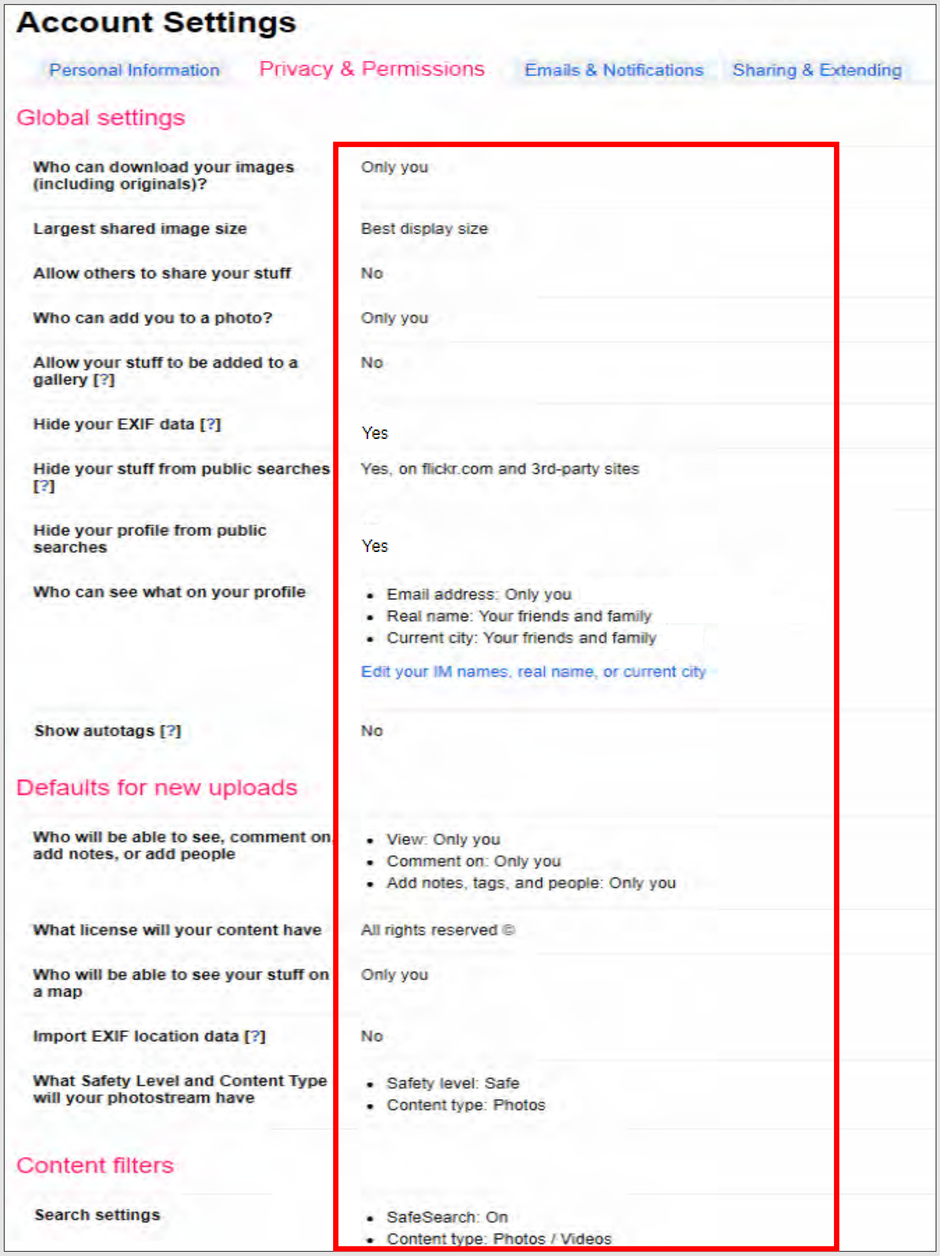
Android devices typically automatically backup photos with your EXIF data, so be sure to check your settings! #KeepGoogleInCheck

PHOTO SHARING SERVICES CARD

With proper security settings Flickr is a great web-based photo storage service, with 1 TB of free storage. #SecureMemories

Privacy Settings Continued

flickr



Account Settings

Personal Information | Privacy & Permissions | Emails & Notifications | Sharing & Extending

Global settings

Who can download your images (including originals)?	Only you
Largest shared image size	Best display size
Allow others to share your stuff	No
Who can add you to a photo?	Only you
Allow your stuff to be added to a gallery [?]	No
Hide your EXIF data [?]	Yes
Hide your stuff from public searches [?]	Yes, on flickr.com and 3rd-party sites
Hide your profile from public searches	Yes
Who can see what on your profile	• Email address: Only you • Real name: Your friends and family • Current city: Your friends and family Edit your IM names, real name, or current city
Show autotags [?]	No

Defaults for new uploads

Who will be able to see, comment on, add notes, or add people	• View: Only you • Comment on: Only you • Add notes, tags, and people: Only you
What license will your content have	All rights reserved ©
Who will be able to see your stuff on a map	Only you
Import EXIF location data [?]	No
What Safety Level and Content Type will your photostream have	• Safety level: Safe • Content type: Photos

Content filters

Search settings	• SafeSearch: On • Content type: Photos / Videos

For a comprehensive Flickr security walkthrough, visit the following URL: https://safety.yahoo.com/SafetyGuides/Flickr/index.htm

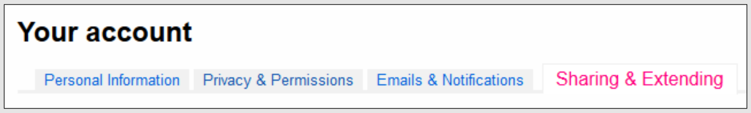
Tap the at the top right corner.

Tap "Settings".

Tap the "Privacy & Permissions" tab and use the image to the left as an example for your security settings.

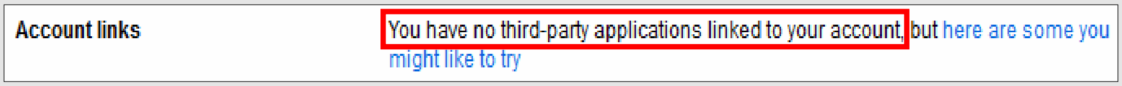
Now tap on the "Sharing & Extending" tab.

Make sure you do not have any third party applications such as Twitter or Tumblr linked to your Flickr account. You should see a message like the one outlined in red below.



Your account

Personal Information | Privacy & Permissions | Emails & Notifications | Sharing & Extending

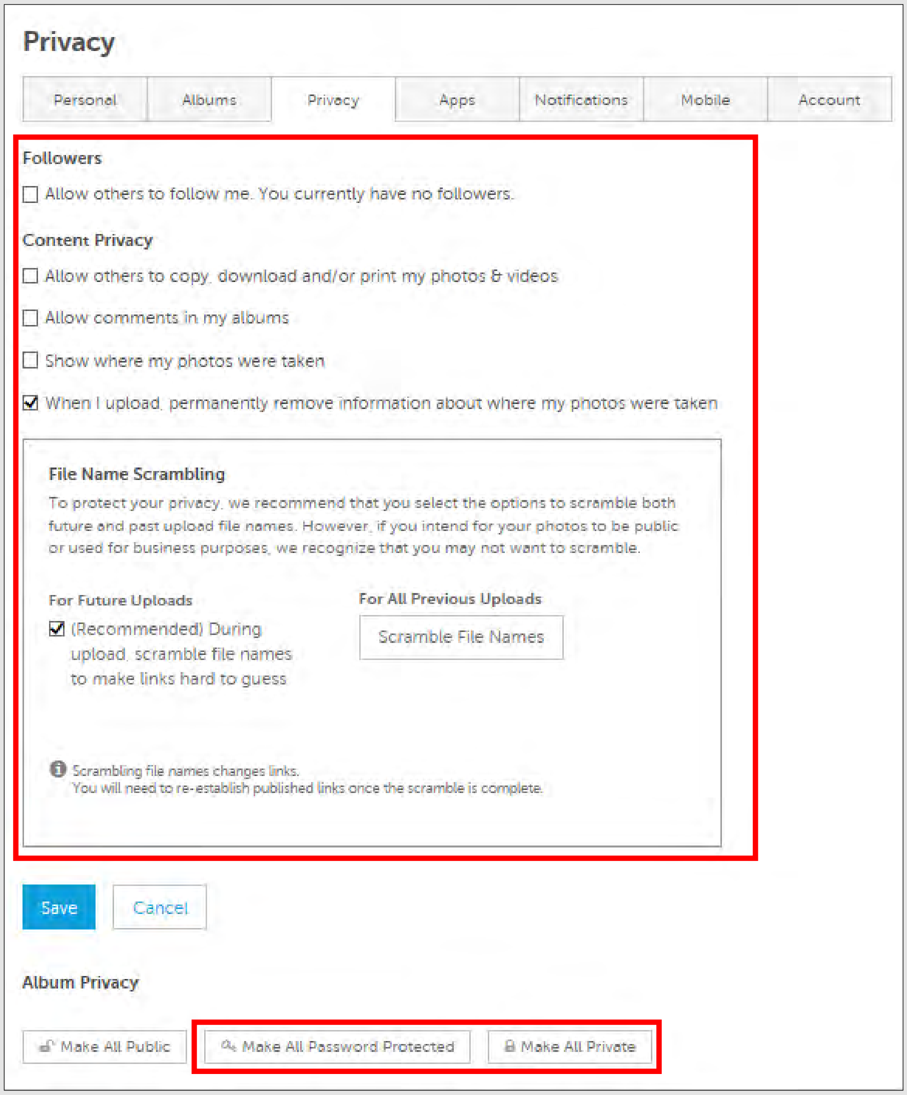


Account links You have no third-party applications linked to your account, but here are some you might like to try

PHOTO SHARING SERVICES CARD

Privacy Settings Continued

photobucket



Privacy

Personal | Albums | Privacy | Apps | Notifications | Mobile | Account

Followers

☐ Allow others to follow me. You currently have no followers.

Content Privacy

☐ Allow others to copy, download and/or print my photos & videos

☐ Allow comments in my albums

☐ Show where my photos were taken

☑ When I upload, permanently remove information about where my photos were taken

File Name Scrambling

To protect your privacy, we recommend that you select the options to scramble both future and past upload file names. However, if you intend for your photos to be public or used for business purposes, we recognize that you may not want to scramble.

For Future Uploads

☑ (Recommended) During upload, scramble file names to make links hard to guess

For All Previous Uploads

Scramble File Names

Scrambling file names changes links.
You will need to re-establish published links once the scramble is complete.

Save | Cancel

Album Privacy

Make All Public | Make All Password Protected | Make All Private

Tap the 👤 at the top right corner.

Tap “Settings”.

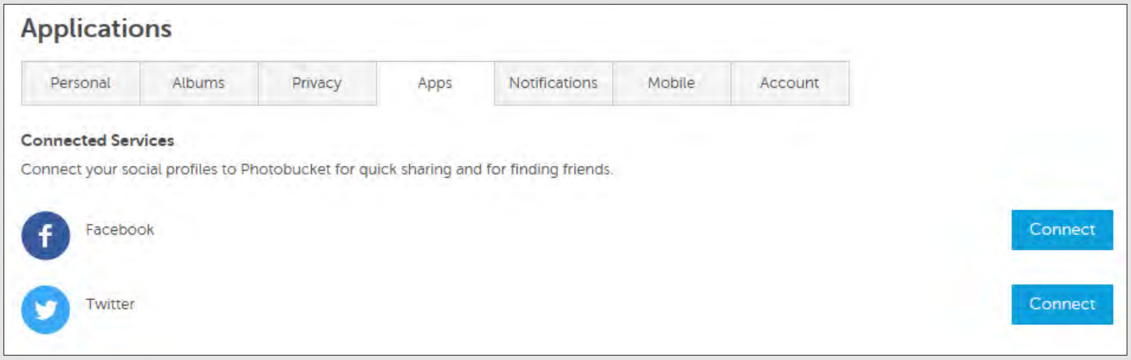
Tap the “Privacy” tab and use the image to the left as an example for your security settings.

Then tap the “Apps” tab.

Make sure you do not have any third party applications such as Twitter or Facebook linked to your Photobucket account.

Safety Fact: Although it is possible to set Photobucket albums to "private," this does not prevent the photos within being accessed by someone who knows or can guess the URL. Internet programs, such as Fuskers, have been created that can identify URL patterns and test for working photo URLs. This allows "private" photos on Photobucket being downloaded and distributed elsewhere on the Internet without the consent of their uploaders.

Photobucket monitors suspicious activity to prevent software from guessing URLs and downloading photos. It is recommended that Photobucket users scramble the links to photos and videos, and select the option to scramble the links of both past and future if there is no need to preserve the original file names.



Applications

Personal | Albums | Privacy | Apps | Notifications | Mobile | Account

Connected Services

Connect your social profiles to Photobucket for quick sharing and for finding friends.

Facebook — Connect

Twitter — Connect

Many photo sharing apps encourage you to link other social media accounts, but with convenience comes increased risk.

UPDATED JAN 2021

SMARTPHONE EXIF REMOVAL SMART CARD

EXIF Data

EXIF—Exchangeable Image File Format—is a standard format for capturing, storing and exchanging image metadata. Metadata is the description and context of files that allows computers to organize, find, and display information about a file. For example, when a music app displays the artist, year, album, and song name of an mp3 being played, it uses the mp3s metadata to display that information. Images and videos also contain metadata that can show time, date, camera settings, copyright information, and location. Some social networks and photo-sharing sites, such as Flickr, Google+, and Dropbox, have features that display EXIF data alongside images. Facebook, Instagram, Twitter and Reddit, do not share EXIF data publicly, but may use the information internally. EXIF metadata are listed as tags that store information that can be used to identify an individual. The chart below shows the tag categories, the metadata included in each category, and the potential security risks associated to each piece of metadata.

Tag Category	Important Tags	Security Implications
Geo-location	GPSLongitude, GPSLongitudeRef, GPSLatitude, GPSLatitudeRef, GPSDateStamp, GPSTimeStamp, GPSAltitude, GPSAltitudeRef, GPSProcessingMethod	Ability to reveal the exact location of private places, such as homes or offices. Some photosharing sites, including Google+ and Flickr, publicly display image GPS coordinates on a map.
Timestamps	ModifyDate, DateTimeOriginal, CreateDate	Creates a log of behavioral patterns and personal timelines.
Camera	Make, Model, Serial Number	A unique serial number identifies the particular device for an image or set of images.
Authorship	Artist, Owner Name, Copyright	Links images with a name or organization.
Image Summary	ImageDescription, UniqueImageID, UserComment	Potentially reveals identifying information about the content of the images, such as captured persons or locations.

Do

- ♦ ***Do*** prevent your device(s) from capturing geo-location data when taking pictures. Remove EXIF metadata from images taken by smartphones or digital cameras.
- ♦ ***Do*** use privacy settings from the app to limit the audience to only yourself or close friends and family, before uploading pictures.
- ♦ ***Do*** assume that anyone can see, copy, or forward photos that are posted online. Even with no EXIF data, the content of images may contain identifying information, including people and locations.

Don't

- ♦ ***Don't*** allow apps to automatically upload and share captured images (e.g. Instagram, Flickr).
- ♦ ***Don't*** assume that device settings remain the same after updates or over time. Verify the settings frequently.
- ♦ ***Don't*** upload pictures with landmarks, easily identifiable structures, or signs indicating location.
- ♦ ***Don't*** give apps used for sharing photos permission to access your device's location or other information.

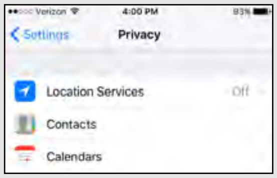
Prevent the Capture of Geolocation Data

iOS

If iOS location services are turned off, images captured with the native iPhone camera app will not contain geo-location EXIF data.

❶ Select the "Settings" app. Click "Privacy" > "Location Services".

❷ Turn off location services altogether or for the iPhone's camera applications.



Verizon 4:00 PM 83%

Settings

Privacy

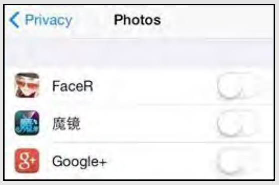
Location Services Off

Contacts

Calendars

❸ Return to the "Settings" app. Click "Privacy" > "Photos".

❹ Disable permissions for other apps to have access to the photos stored in the device's camera roll.



Privacy

Photos

FaceR

魔镜

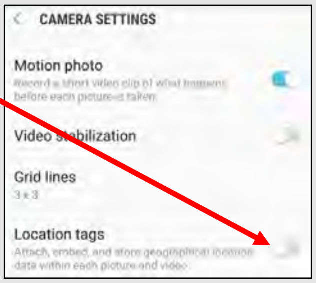
Google+

Android

Turning off location storage in the Android camera application prevents captured images from containing EXIF data.

❶ Open the camera app and go to "Settings" by tapping the gear icon. This varies from phone to phone since there is no standard camera app on Android devices.

❷ After that, scroll down until you see 'location tags' and touch the toggle switch to disable geotagging of photos. The wording may vary slightly between devices.



CAMERA SETTINGS

Motion photo

Record a short video clip of what happens before each picture is taken

Video stabilization

Grid lines

3 x 3

Location tags

Attach, embed, and store geographical location data within each picture and video

Twitter doesn't share your EXIF data, but it will geo-tag your post if location services are enabled. #DisableLocationServices

UPDATED JAN 2021

SMARTPHONE EXIF REMOVAL SMART CARD

Prevent the Capture of Geolocation Data Continued

- Taking a screenshot of a photo on a device running iOS or Android will create a new image containing no EXIF data. To take a screenshot on an iOS device, simultaneously press the lock and home buttons or google how to take a screenshot on your specific android.
- Even photos taken in airplane mode contain geo-location data. It is recommended to turn off location services/ storage on your smartphone camera application, as shown on the previous page.
- Remember that uploading or sharing a lower quality image will contain EXIF data. EXIF data and image quality have no correlation.
- It is important to not only lock down Apps such as Snapchat, Instagram and Twitter (see corresponding Smartcard), but to also remove the meta data from them as best as possible.

EXIF Removal Apps and Programs

Reviewing & Removing EXIF Data for iOS

1. Download the free US-based Photo Investigator app from the App Store.
2. Open the app and tap the gallery icon on the bottom left.
3. To view EXIF data, you can tap on the various icons below the image.
4. To remove EXIF data tap “Metadata” and then select “Remove”.

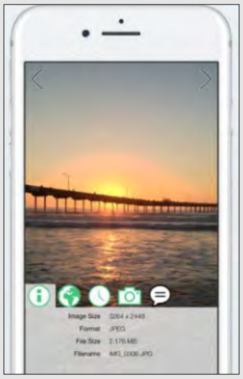


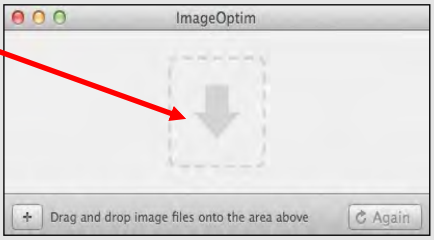
Image Size	3264 x 2448
Format	JPEG
File Size	2.176 MB
Filename	IMG_0006.JPG

5. An easy way to identify photos that have EXIF data with geo-locations is to view your “Places” folder. Any images that appear in this folder have geolocation data, once you disable the geotagging feature and remove your EXIF data, this folder should be empty.

Reviewing & Removing EXIF Data in macOS

Use the Image Optim (UK based) application (available at http://imageoptim.com/) to remove EXIF data on your OS X device.

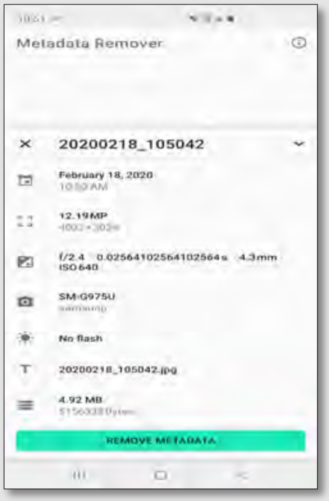
1. Drag the photos for EXIF removal into the app window and wait for a green check mark to appear next to the file name.



2. Check that the EXIF data has been removed by right clicking the image and selecting “Get Info”. EXIF data is listed under “More Info”.

Metadata Remover for Android

Metadata Remover is a free US-based app that deletes all EXIF data from image files stored on your Android device.



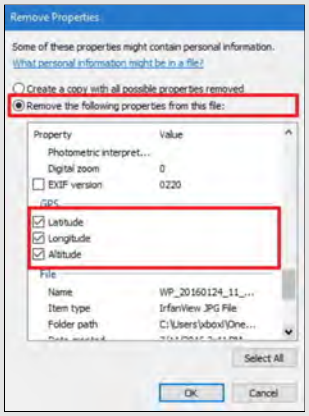
20200218_105042
February 18, 2020
10:50 AM
12.19MP
4000 × 3024
f/2.4 0.02564102564102564s 4.3mm
ISO 640
SM-G975U
samsung
No flash
20200218_105042.jpg
4.92 MB
5156338 bytes

1. Download a Photo Exif Editor app from the Play Store.
2. Open the app and select an image.
3. The EXIF data will be removed.
4. Processed images will be saved separately from the original file.

Reviewing & Removing EXIF Data in Windows

Use the Windows OS to verify EXIF data has been removed.

1. Navigate to an image in File Explorer. Right click the image and select “Properties”.
2. Select the “Details” tab. You can examine EXIF metadata that is available.
3. Click “Remove Properties and Personal Information”.
4. You can click “Create a copy with all possible properties removed” to remove all potential properties or select individual properties such as GPS information. Click “OK”.



Remove Properties

Some of these properties might contain personal information.
What personal information might be in a file?

○ Create a copy with all possible properties removed
● Remove the following properties from this file:

Property	Value
Photometric interpret...	
Digital zoom	0
□ EXIF version	0220
GPS	
☑ Latitude	
☑ Longitude	
☑ Altitude	
File	
Name	WP_20160124_11_...
Item type	IrfanView JPG File
Folder path	C:\Users\xboxl\One...

Geo-localization

Even with EXIF metadata removed, images containing vegetation, addresses, business names, road markings, and landmarks allow someone to identify the location a photograph was taken. Geo-localization, the determination of a location of an image through visual information, is currently being developed. This will allow computers to compare a picture without EXIF metadata to millions of other picture found on the internet that do have location metadata. Once the computer discovers a close match between two pictures, it can apply the location metadata of one structure to its match that does not have location metadata.

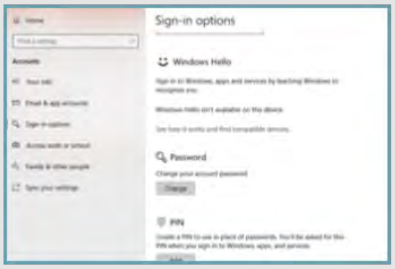
Remove EXIF data before sharing or posting images, especially images captured in private homes or businesses. #PhotoSafety

UPDATED JAN 2021

LOCK DOWN YOUR LAPTOP SMART CARD

Creating a Windows Log-in Password

Although a log-in password won't protect against a competent hacker, it can be enough to dissuade unsophisticated criminals from snooping through your personal files and accessing your online accounts. Protecting each account (Guest, Admin, and User) with different passwords helps prevent a hacker from getting access to everything on your computer should they gain access to any one account. It is recommended you create and use a "User" account, not the "Admin" account for all daily activity. This way hackers would be limited in the damage they can do to your computer.



Sign-in options

Windows Hello

Sign in to Windows, apps and services by teaching Windows to recognize you.

Windows Hello isn't available on this device.

See how it works and find compatible devices.

Password

Change your account password

Change

PIN

Create a PIN to use in place of passwords. You'll be asked for this PIN when you sign in to Windows, apps, and services.

Windows 10 offers a number of enhanced log-in and security features.

Navigate to **Start Button > Settings > Accounts > Sign-in Options** to setup your 'Sign-in Options".

Practical Password Tips

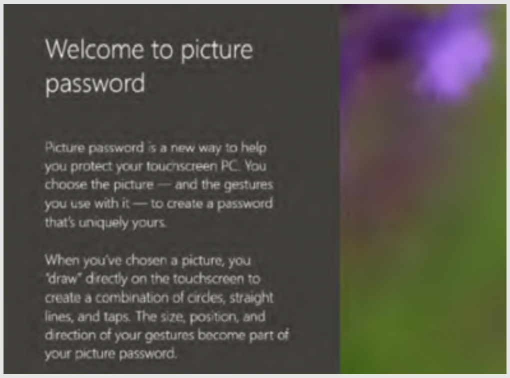
If you have files on your computer that you don't want anyone else to access, you can use password-protected file or folder encryption to keep them safe. However, encrypted files are only as secure as the strength of the password protecting them.

For this and the rest of your security measures to be maximally effective, make sure you follow these simple password rules:

- Use a password that's at least 12 characters long and includes a mix of lower and upper case letters, symbols, and numbers. Try not to use complete words, but if necessary avoid common words that can be found in a dictionary. Not all devices, systems, or accounts allow these combinations, but do what you can within the available options.
- Avoid sharing passwords across multiple platforms, especially for sensitive accounts like a Windows logon, bank account, and email account.
- Change your passwords frequently - every 6 months for important passwords, at a minimum.

Additional Security

Windows 10 also has a number of additional log-in security features. At the "Settings," "Accounts" and "Sign-in Options" menu you can select "Picture Password" to enable secure log-in based on your unique mouse movement responses.



Welcome to picture password

Picture password is a new way to help you protect your touchscreen PC. You choose the picture — and the gestures you use with it — to create a password that's uniquely yours.

When you've chosen a picture, you "draw" directly on the touchscreen to create a combination of circles, straight lines, and taps. The size, position, and direction of your gestures become part of your picture password.

Note: You can use a PIN to sign into Windows, apps, and services. However, this option is not as secure as the "Picture Password."

Windows 10 also has a feature which allows you to pair your laptop with a Bluetooth-enabled device and automatically lock your computer once the device is out of range. You can enable this feature from the "Settings," "Accounts" and "Sign-in Options" menu by pairing your laptop to a Bluetooth device with the "Dynamic Lock" slider.

For personal accounts you can also enable two-factor authentication (2FA). 2FA requires users to authenticate access through a supported device, i.e. a text to a phone number or an email to a backup address, before accessing an account.

Encryption Basics

Some versions of Windows 10 allow users to easily encrypt file, folder and hard drive data with BitLocker protection. To access BitLocker, navigate to "Control Panel", "System and Security" and select the BitLocker slider or "Device Encryption" to secure your hard drive data. Some newer devices are encrypted by default, which may be the case if you are unable to locate a Bitlocker option on your device. If you'd rather use "on-the-fly" software to lock certain files or folders, you can also use a number of Freeware (Free Software) encryption services such as VeraCrypt, AxCrypt, GNU Privacy Guard, or 7-Zip. You can find these tools and other simple encryption tips at: lifehacker.com/five-best-file-encryption-tools-5677725

Laptop Security Tip: If possible, set-up two factor authentication on your laptop by pairing it with a Bluetooth device you carry on your person.

UPDATED JAN 2021

LOCK DOWN YOUR LAPTOP SMART CARD

Virtual Private Network (VPN)

A Virtual Private Network (VPN) connection is the safest way to connect to the Internet and also safeguard your information.

Unsecured networks present a major threat to your personal information, especially when using your device on a public WIFI network. When connecting to public WIFI, we don’t know who else is on the local network, which leaves our personal data vulnerable to snooping. Even when connecting to the wider web, our data is increasingly collected, inspected and exploited.

One sensible solution is to use a VPN. We recommend using a VPN whether you are connecting to the internet from home (even with a secure WIFI connection) or in public. This is simply the most secure way to access the Internet.

VPN For Beginners

When you connect to a VPN, you access a site or service directly from your laptop, which acts as a secure launchpad into the World Wide Web. Once connected to the service, your data is encrypted and sent to a third-party server. There it is combined with other traffic before being integrated into the “normal” traffic flow on the World Wide Web. Since your information is jumbled up with other information, it becomes difficult to identify as *your* specific information, it is like a needle in a haystack.

A Few VPN Perks

- VPN services are cheap, with some starting around $5 per month.
- A VPN can help protect your data from identity theft and fraud.
- VPN providers often allow users significantly increased privacy protections from advertisers and hackers alike.
- VPN providers allow you to enjoy services that require connections from certain countries, regions or time zones.
- If your Internet Service Provider blocks some applications, such as Skype or other VoIP (Voice over Internet Protocol) applications, use of a VPN may help.

Where To Find VPN Services

Not all VPN services are created equal. Depending on your typical Web usage, you will want to shop around for a service that fits your profile. If you need a fast connection for rapid-fire browsing or streaming services and your VPN provider doesn't have enough servers, you may experience poor Internet speeds or be unable to make a connection at all. Others might offer some privacy protections but require you to give up some control of your anonymity.

Before subscribing to a VPN service, be sure to look at reviews. The VPN market is competitive and expanding which means VPN providers often offer free trial periods to new users.

For additional information on current VPN providers see: www.pcmag.com/article2/0,2817,2403388,00.asp

Sources

http://www.pcworld.com/article/2025897/a-road-warriors-guide-to-locking-down-your-laptop.html
https://www.umass.edu/it/support/security/laptop-mobile-device-physical-security-dos-donts
http://www.pcworld.com/article/2308725/encryption/a-beginners-guide-to-bitlocker-windows-built-in-encryption-tool.html
http://www.lehman.edu/itr/documents/computer-security-dos-donts.pdf
http://www.pcworld.com/article/223044/vpns_for_beginners_to_experts.html
https://laptop.ninja/5-dos-and-donts-for-laptop-owners/
https://www.pcmag.com/feature/358289/two-factor-authentication-who-has-it-and-how-to-set-it-up

Laptop Security Tip: Full-disk encryption can protect your data but only when used in combination with good password security practices.

UPDATED JAN 2021

SECURING YOUR HOME WIRELESS NETWORK

Best Practices

- Create passwords that are sufficiently long and complex to include; upper and lowercase letters, numbers, and symbols. Consider a multi-password phrase that does not consist of dictionary-based words. An example would be ILuvF00tb@77 from the phrase "I love football."
- Use a cable to directly connect any stationary computers / devices to your home network to limit vulnerabilities presented by wirelessly connected devices
- Turn off your wireless network when you will not be using it for an extended period of time.
- If you have guest-access set up for your network, ensure that it is also password protected.
- If possible, turn on automatic updates for your network device's firmware. If they are not offered, periodically check for firmware updates on the network devices' website(s) and manually download and install them.
- If your router is compromised or if you cannot remember the password, you can restore it to the default factory settings by pressing the reset button usually located on the back of the router.
- Position the router away from windows and as far into the interior of your house as possible to limit the range of the WiFi signal outside your home.

Glossary of Commonly Used Terms

Wireless Router	Physical hardware that allows users to connect their devices to a shared internet network.
Service Set Identifier (SSID)	Public name of a wireless network.
Pre-Shared Key (PSK)	Authentication mechanism that mandates a password. Adds additional security to wireless networks.
Hypertext Transfer Protocol Secure (HTTPS)	Uses various encryption protocols to add additional security to HTTP.
Media Access Control (MAC) Address	Unique, individual identifier assigned to computers and devices.

Wi-Fi Security Level	Level of Security	Explanation
WEP	Low/Risky	Old encryption protocol. No longer considered a standard. Highest risk next to an "open" network.
WPA	Low-Moderate	Older encryption protocol. Better than WEP but should not be used when more modern encryption (WPA2) is available.
WPA2	Moderate-high	WPA2-PSK (AES) is the most secure option which uses the latest Wi-Fi encryption.
WPA3	High	Approved and replacing WPA2 by the end of 2018, as the new and more secure option for Wi-Fi Security.

Accessing Your Router

In order to change your WPA2 password you will need to access your router. In order to access your router, you must enter the appropriate IP address, username, and password. If you do not have this information, your Internet Provided should be able to provide it to you.

It is **important** to understand that when your internet is being set up by your Internet Provider, they are not required to set it up using WPA2 (see the chart to the left). Recommend you ensure they set it up for you and provide the IP address for the router's settings. That way, once they leave you can change the user name and password.

When changing your username and password for the WIFI, it is important to consider the following: choose a username that does not include you or your family members' names; create a password that is long and complex. Lastly, it is important to change any "Guest Account" password to something other than your "Admin/Family Account" password.

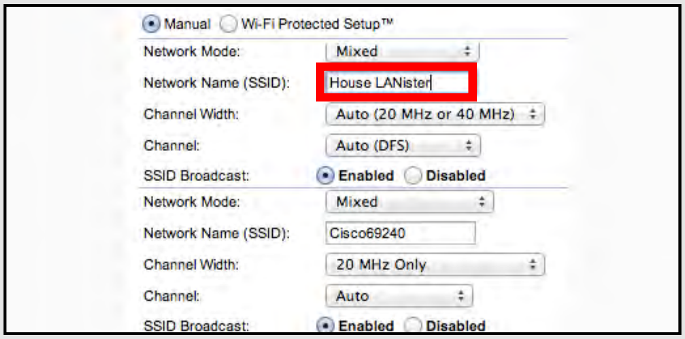
Passwords provided by your internet provider are general in use; it is a good idea to change the password after everything is set up. #keepyourhomesecure

UPDATED JAN 2021

SECURING YOUR HOME WIRELESS NETWORK

Even if you have set up WPA2-PSK on your WI-FI it is still very important to have a virus and malware protection for your computer. #cybersecurity

Creating a Unique SSID



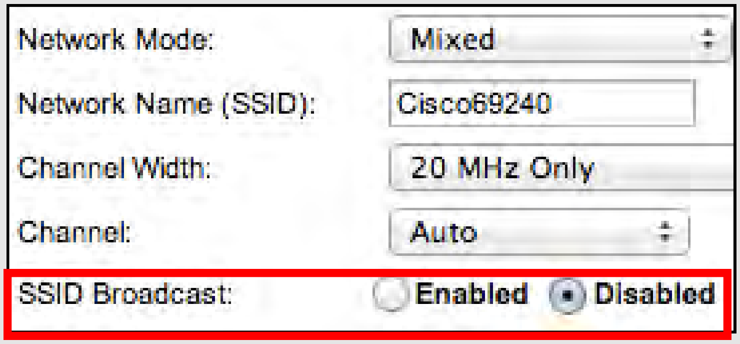
● Manual ○ Wi-Fi Protected Setup™

Network Mode: Mixed
Network Name (SSID): House LANister
Channel Width: Auto (20 MHz or 40 MHz)
Channel: Auto (DFS)
SSID Broadcast: ● Enabled ○ Disabled

Network Mode: Mixed
Network Name (SSID): Cisco69240
Channel Width: 20 MHz Only
Channel: Auto
SSID Broadcast: ● Enabled ○ Disabled

When creating a name for your Wi-Fi (your SSID), it is important to consider who will be seeing it and what information it may give away about you and your family. For instance, if you decide to give it the family name (last name and perhaps number of family members), then anyone within range will be able to see your last name and likely piece together what the numbers represent. Alternately, if you name your SSID "FBI Van," that may call attention to your specific network and entice nefarious individuals into attempting to hack into it. It is recommended that you choose a name for your SSID that is generic in nature, providing no information about your family, address, date of birth, etc.

Disabling the SSID Broadcast



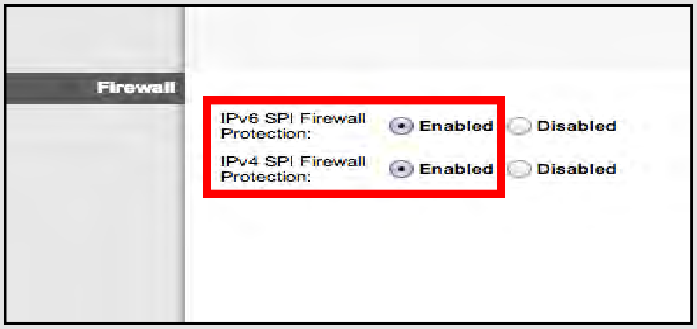
Network Mode: Mixed
Network Name (SSID): Cisco69240
Channel Width: 20 MHz Only
Channel: Auto
SSID Broadcast: ○ Enabled ● Disabled

If you would like to hide your SSID so that it does not broadcast to the public, you can do so by scrolling down from where you created your SSID name till you find what's pictured above. Note that, while it is nice to be able to disable the broadcasting of your SSID, it can be "unhidden" by any individual requesting "hidden Wi-Fi's".

Children's Learning Devices: If you have smaller children in your home who have devices like the Leapfrog or Vtech games, and you disable your SSID broadcasting, these devices will not be able to locate your WIFI network and connect to the internet. In order for these devices to connect, you need to go back into your router settings and "Enable" the broadcasting of your SSID.

The next two settings are usually found in "Router Settings" but you may have to look around a bit to find them.

Router Firewall



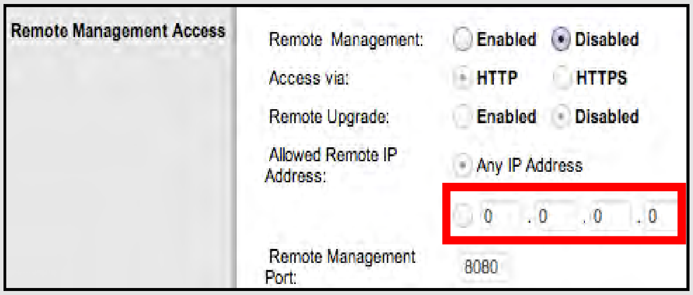
Firewall

IPv6 SPI Firewall Protection: ● Enabled ○ Disabled
IPv4 SPI Firewall Protection: ● Enabled ○ Disabled

A "Firewall" is a layer of security between your home network and the Internet. Since a router is the main connection from a home network to the Internet, the firewall function is merged into the router. Every home network should have a firewall to protect its privacy.

A firewall does not secure against every kind of attack. For example, you still need to run a virus-checker on all your computers.

Remote Access



Remote Management Access

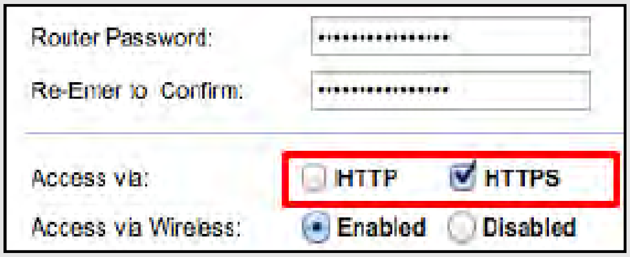
Remote Management: ○ Enabled ● Disabled
Access via: ● HTTP ○ HTTPS
Remote Upgrade: ○ Enabled ● Disabled
Allowed Remote IP Address: ● Any IP Address
○ 0 . 0 . 0 . 0
Remote Management Port: 8080

Check that the Remote Management IP Address is set to **0.0.0.0** to ensure that remote access is disabled. This will help to ensure that others cannot access your router remotely and without your permission.

UPDATED JAN 2021

SECURING YOUR HOME WIRELESS NETWORK

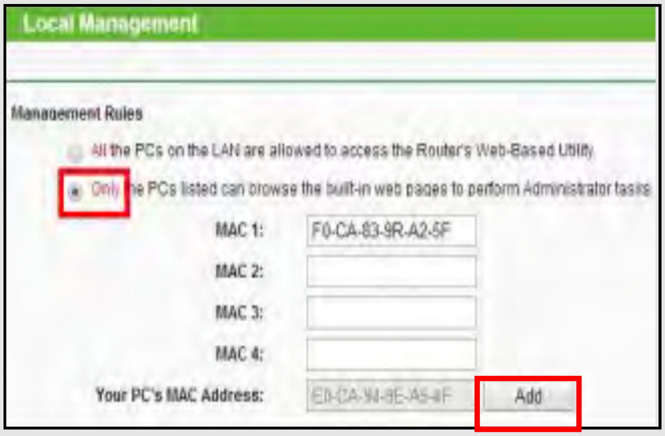
Enabling HTTPS



Router Password:	••••••••••••••••
Re-Enter to Confirm:	••••••••••••••••
Access via:	□ HTTP ☑ HTTPS
Access via Wireless:	● Enabled ○ Disabled

HTTPS is a variant of the standard web transfer protocol (HTTP) that adds a layer of security on the data in transit. HTTPS enables encrypted communication and secure connection while on the internet. It is used by websites to provide enhanced security for customers OR financial transactions OR where personally identifiable information (PII) is shared. Enabling HTTPS on your servers is a critical step in providing security for your web pages. It is recommended that you enable HTTPS in order to further protect you and your family while navigating the internet.

Wireless MAC Filtering



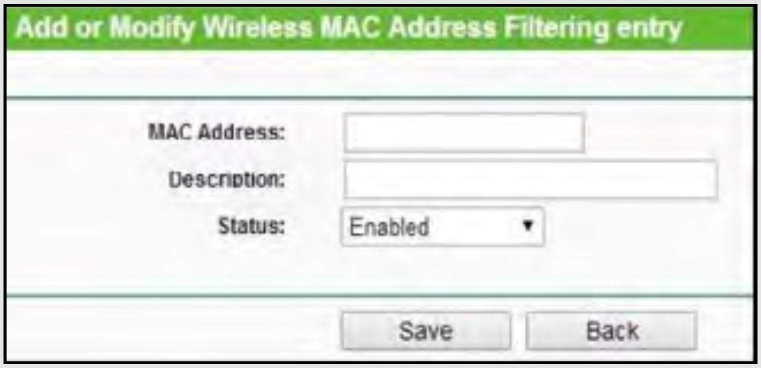
Local Management

Management Rules

○ All the PCs on the LAN are allowed to access the Router's Web-Based Utility

● Only the PCs listed can browse the built-in web pages to perform Administrator tasks

MAC 1:	F0-CA-83-9R-A2-5F
MAC 2:	
MAC 3:	
MAC 4:	
Your PC's MAC Address:	E0-CA-94-9E-A5-4F

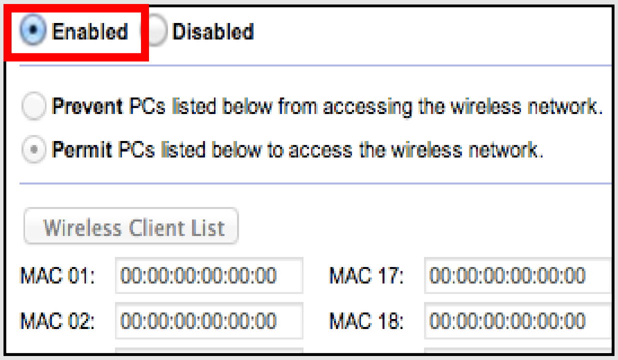


Add or Modify Wireless MAC Address Filtering entry

MAC Address:	
Description:	
Status:	Enabled

MAC address filtering allows you to define a list of devices' MAC addresses so that only those devices can access your Wi-Fi. In order to do so, follow the steps below:

Add the MAC address of each device you want to authorize access to your network (as highlighted above). Next, enter the MAC address and a brief description of the connected device for filtering. Finally, enable MAC address filtering to ensure that only approved computers and devices can connect to your router (as highlighted in the box to the right). Click the 'Add' button when done entering authorized devices.



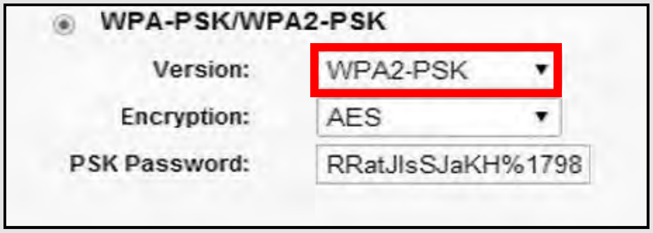
● Enabled ○ Disabled

○ Prevent PCs listed below from accessing the wireless network.

● Permit PCs listed below to access the wireless network.

MAC 01:	00:00:00:00:00:00	MAC 17:	00:00:00:00:00:00
MAC 02:	00:00:00:00:00:00	MAC 18:	00:00:00:00:00:00

Encryption



● WPA-PSK/WPA2-PSK

Version:	WPA2-PSK
Encryption:	AES
PSK Password:	RRatJlsSJaKH%1798

Between the optional WEP, WPA, WPA-PSK, WP2, and WPA2-PSK algorithms, you should select WPA2-PSK and also AES (a cryptographic cipher that is responsible for a large amount of the information security that you enjoy on a daily basis) for encryption. The PSK password should be long and complex, but different from the administrative router-access password.

Useful Links

Practically Networked
www.practicallynetworked.com/support/wireless_secure.htm

Wi-Fi.org
www.wi-fi.org/discover-wi-fi/security

Routers need to be updated. We tend to take our Wi-Fi for granted, but just like taking the car in for an oil change we need to patch routers routinely. #themoreyouknow

UPDATED JAN 2021

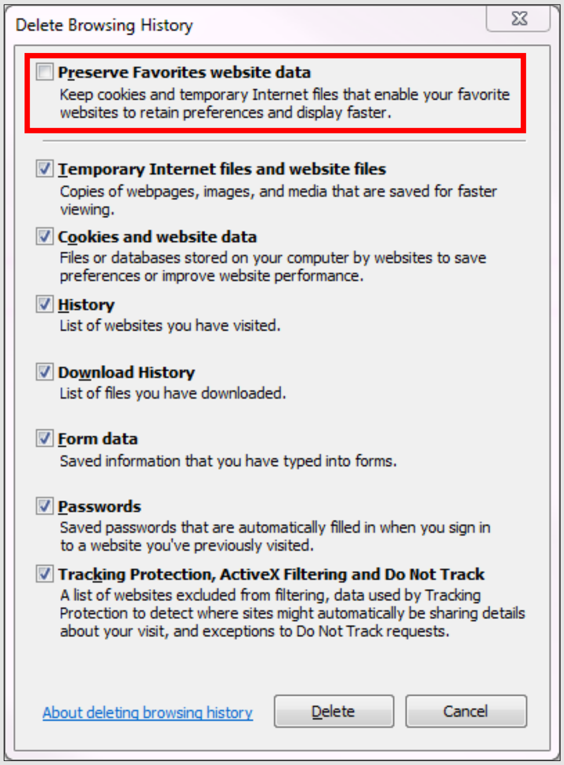
DELETE BROWSER ARTIFACTS SMART CARD

Browser Artifacts—Cookies, Cache & History

Information such as browsing history, cache, and cookies are saved on your computer while you surf the Web. They are used in various ways to improve your browsing experience. These private data components, while resulting in conveniences such as faster load times and auto-populated fields, can be used by nefarious actors. Whether it be the password for your email account or your credit card number and address, much of the data left behind at the end of your browsing session could be dangerous in the wrong hands. In order to protect yourself, we recommend you delete these artifacts on a regular basis.

An internet cookie is a small piece of data sent from a website and stored on a user's computer while the user is browsing.

Deleting Internet Explorer Web Browser Artifacts



Delete Browsing History

☐ **Preserve Favorites website data**
Keep cookies and temporary Internet files that enable your favorite websites to retain preferences and display faster.

☑ **Temporary Internet files and website files**
Copies of webpages, images, and media that are saved for faster viewing.

☑ **Cookies and website data**
Files or databases stored on your computer by websites to save preferences or improve website performance.

☑ **History**
List of websites you have visited.

☑ **Download History**
List of files you have downloaded.

☑ **Form data**
Saved information that you have typed into forms.

☑ **Passwords**
Saved passwords that are automatically filled in when you sign in to a website you've previously visited.

☑ **Tracking Protection, ActiveX Filtering and Do Not Track**
A list of websites excluded from filtering, data used by Tracking Protection to detect where sites might automatically be sharing details about your visit, and exceptions to Do Not Track requests.

About deleting browsing history

Delete

Cancel

Make sure you are using the latest version of Internet Explorer (IE), IE 11.

Click the Settings ⚙ button on the top right.

Click "Internet Options".

Under the "General" tab, locate the "Browsing History" section.

Click "Delete".

You will see the window to the left. (A useful keyboard shortcut to access this window is "*Ctrl-Shift-Delete").*

Deselect "Preserve Favorites website data".

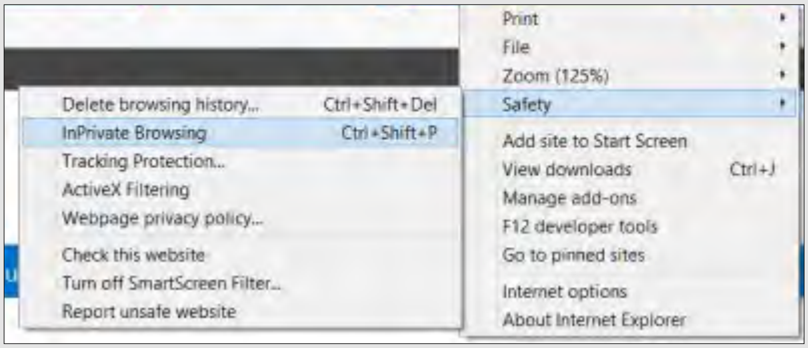
Select the boxes next to the history you want to remove and click "Delete".

Exit/quit all browser windows and re-open the browser.

Note: Internet Explorer is no longer supported on any mobile device.

As of March 2017, Microsoft announced that Microsoft Edge would replace Internet Explorer as the default browser on its Windows 10 devices. As of February 2020, IE version 10 is no longer in support. If you are still using IE be sure to upgrade to IE 11.

Using Internet Explorer InPrivate Browser



To activate "InPrivate", click the Settings ⚙ button on the top right.

Click "Safety".

Click "InPrivate Browsing".

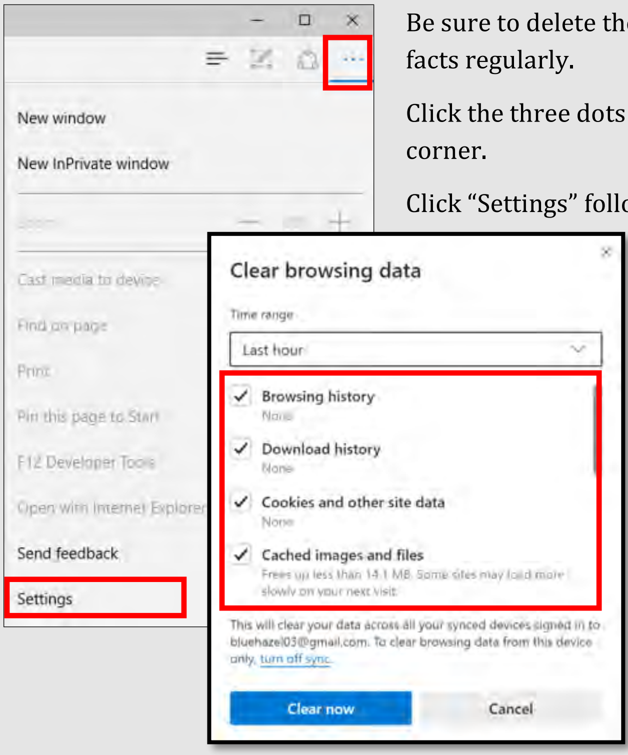
(Alternatively, after opening Internet Explorer you can use the shortcut "*Ctrl-Shift-P*").

UPDATED JAN 2021

DELETE BROWSER ARTIFACTS SMART CARD

An internet cookie is a small piece of data sent from a website and stored on a user's computer while the user is browsing.

Deleting Microsoft Edge Web Browser Artifacts



Clear browsing data

Time range

Last hour

☑ Browsing history
None

☑ Download history
None

☑ Cookies and other site data
None

☑ Cached images and files
Frees up less than 14.1 MB. Some sites may load more slowly on your next visit.

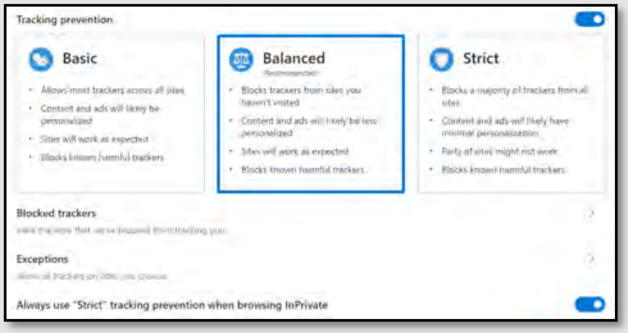
This will clear your data across all your synced devices signed in to bluehazel03@gmail.com. To clear browsing data from this device only, turn off sync.

Clear now | Cancel

Be sure to delete the browser artifacts regularly.

Click the three dots at the top right corner.

Click "Settings" followed by the "Privacy, search, and services" tab.



Tracking prevention

Basic
- Allows most trackers across all sites
- Content and ads will likely be personalized
- Sites will work as expected
- Blocks known harmful trackers

Balanced
Recommended
- Blocks trackers from sites you haven't visited
- Content and ads will likely be less personalized
- Sites will work as expected
- Blocks known harmful trackers

Strict
- Blocks a majority of trackers from all sites
- Content and ads will likely have minimal personalization
- Parts of sites might not work
- Blocks known harmful trackers

Blocked trackers
View the sites that we've blocked from tracking you

Exceptions
Allow all trackers on sites you choose

Always use "Strict" tracking prevention when browsing InPrivate

Select "Tracking prevention," recommend selecting the "Balanced" tracking selection.

Then click "Choose what to clear" under "Clear Browser Data".

Select the boxes next to the history you want to remove and click "Clear".

Mobile Browser

Open the Edge browser.

Tap the menu button on the top right.

Tap to view history.

Tap to clear all history.

Choose the types of data to remove from your phone and tap "Clear".

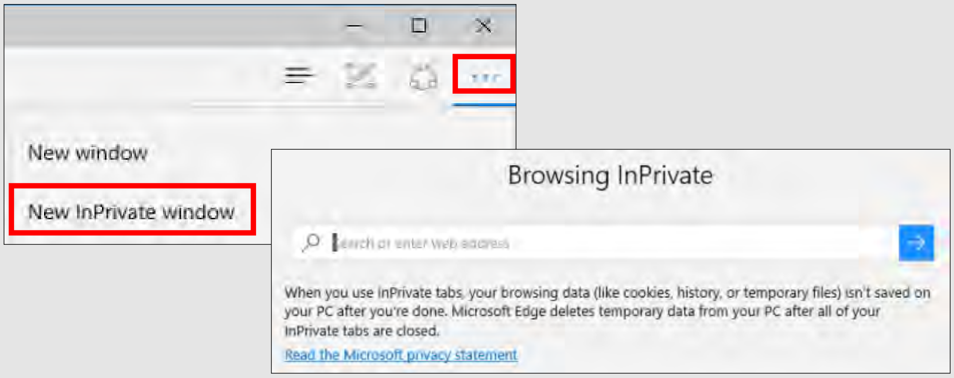
Using Microsoft Edge InPrivate Browsing

Edge is Microsoft's new browser that comes with Windows 10. It is meant to eventually replace IE.

Edge comes with an option called "InPrivate", which is the browser's private mode that does *not* record your activities.

To activate "InPrivate", click the three dots in the browser's upper right corner.

Click "New InPrivate window".



Browsing InPrivate

Search or enter web address

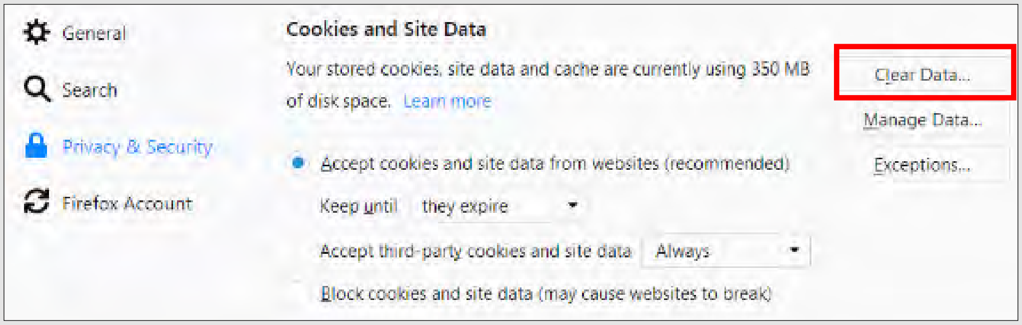
When you use InPrivate tabs, your browsing data (like cookies, history, or temporary files) isn't saved on your PC after you're done. Microsoft Edge deletes temporary data from your PC after all of your InPrivate tabs are closed.

Read the Microsoft privacy statement

UPDATED JAN 2021

DELETE BROWSER ARTIFACTS SMART CARD

Deleting Firefox Web Browser Artifacts



Cookies and Site Data

Your stored cookies, site data and cache are currently using 350 MB of disk space. Learn more

● Accept cookies and site data from websites (recommended)

Keep until: they expire

Accept third-party cookies and site data: Always

○ Block cookies and site data (may cause websites to break)

Click the menu button at the top right and click “Options”.

Click “Privacy & Security” on the left.

Then click “Clear Data”.

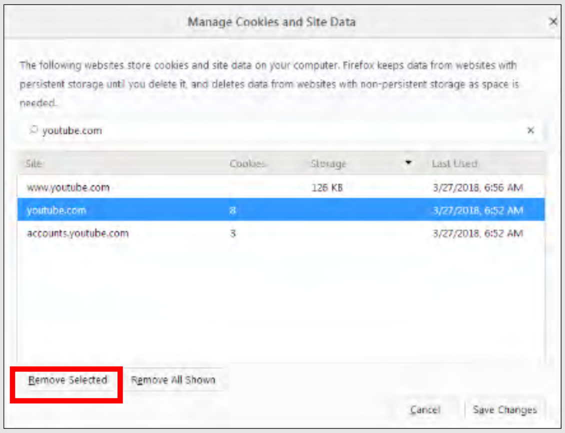
Individual Cookies

You can also remove individual cookies.

From the “Privacy & Security” screen, click “Manage Data”.

Select the site(s) you wish to clear data for.

Then click “Remove Selected”.



Manage Cookies and Site Data

The following websites store cookies and site data on your computer. Firefox keeps data from websites with persistent storage until you delete it, and deletes data from websites with non-persistent storage as space is needed.

youtube.com

Site	Cookies	Storage	Last Used
www.youtube.com		126 KB	3/27/2018, 6:56 AM
youtube.com	8		3/27/2018, 6:52 AM
accounts.youtube.com	3		3/27/2018, 6:52 AM

Mobile Browser

Tap the Menu icon on the top right.

Tap “Settings”. Scroll down to “Clear Private Data” and tap it.

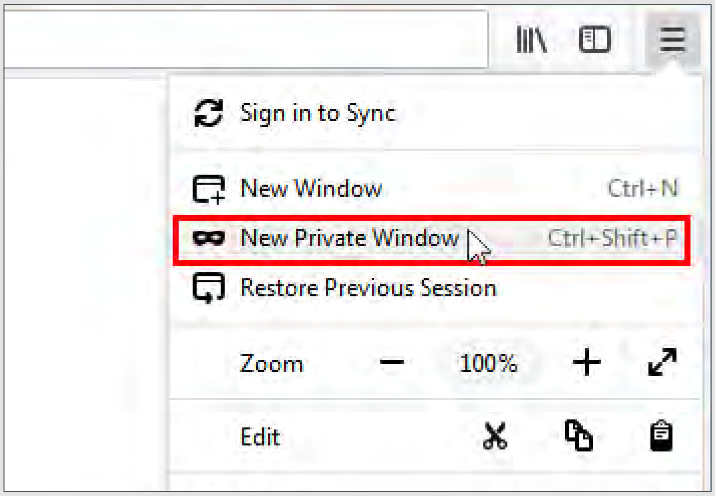
Selected data to be cleared. Tap “Clear Data.”

To manage how your data is shared and tracked, tap “Privacy” then tap “Tracking Protection” from the Settings menu.

“Enabled In Private Browsing” will inform sites that you do not want your browsing behavior tracked, but honoring this is voluntary.

Cookies can also be disabled from this screen.

Using Firefox Private Browsing Mode



To open a new Private Window, click the menu button on the top right.

Click “New Private Window”.

Alternatively, after opening Firefox you can use the shortcut “*Ctrl-Shift-P*”.

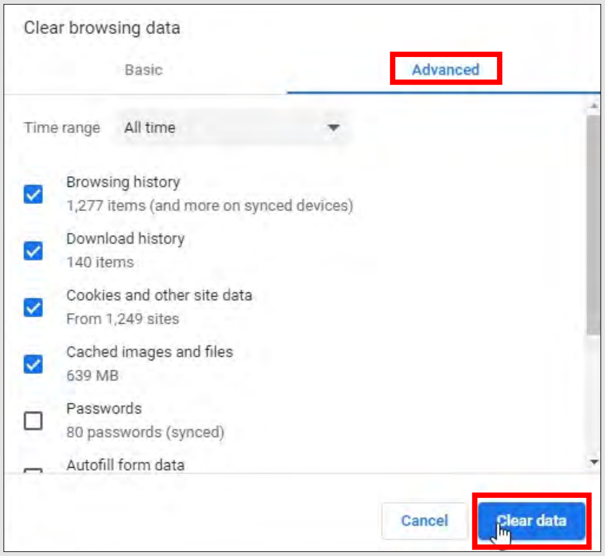
Important: Private Browsing doesn't make you anonymous on the Internet. Your Internet service provider, employer, or the sites themselves can still track what pages you visit. Private Browsing also doesn't protect you from keyloggers or spyware that may be installed on your computer.

Private Browsing also includes Tracking Protection, which prevents companies from tracking your browsing history across multiple sites.

UPDATED JAN 2021

DELETE BROWSER ARTIFACTS SMART CARD

Delete Google Chrome Browser Artifacts



Clear browsing data

Basic | Advanced

Time range: All time

☑ Browsing history
1,277 items (and more on synced devices)

☑ Download history
140 items

☑ Cookies and other site data
From 1,249 sites

☑ Cached images and files
639 MB

☐ Passwords
80 passwords (synced)

☐ Autofill form data

Click the ⋮ icon at the upper right corner.

Click “History” or hold *Ctrl-H*.

Click “History” again on the menu on the upper left hand side.

Click “Clear Browsing Data”. You can also hold C*trl-Shift-Delete*.

Click the “Advanced” tab in the pop-up window.

Select the Time range you desire.

Select the boxes next to the history you want to remove and click “Clear Browsing Data”.

Exit/quit all browser windows and re-open the browser.

Mobile Browser

Tap the menu ⋮ icon.

Then tap “Settings”.

Tap “Privacy and security”.

Tap “Clear Browsing Data”.

Select the boxes next to the history you want to remove and tap “Clear Data”.

Individual Cookies

You can also remove individual cookies.

Click the ⋮ icon at the upper right corner.

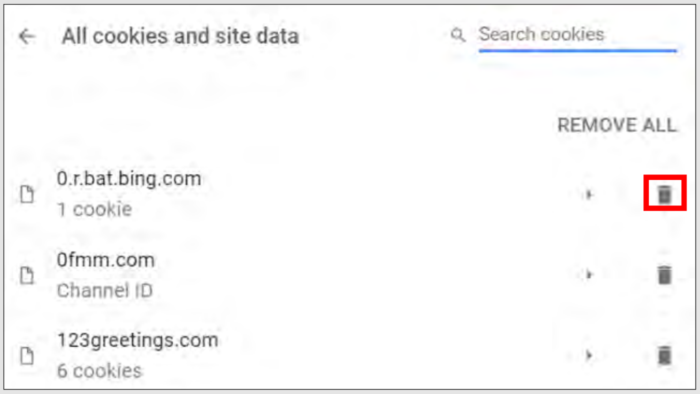
Click “Settings”.

Click the “Advanced” button on the left hand side.

Under the “Privacy & Security” section, click the “Site Settings”.

Click “Cookies and site data” and then “See all cookies and Data”.

Click 🗑 for the sites you wish to clear.



All cookies and site data

0.r.bat.bing.com
1 cookie

0fmm.com
Channel ID

123greetings.com
6 cookies

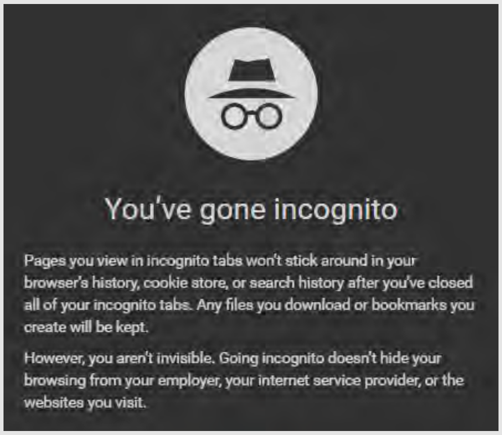
Using Google Chrome Incognito Mode

Chrome’s Incognito mode will *not* save a record of what you visited or downloaded.

Be aware that Incognito is not available if you are using Window 10’s “Family Mode.”

Click the ⋮ icon at the upper right. Select “New Incognito Window”.

You can also use Incognito via the Chrome app on your iOS or Android device. Follow the same steps as above with the app.



You've gone incognito

Pages you view in incognito tabs won't stick around in your browser's history, cookie store, or search history after you've closed all of your incognito tabs. Any files you download or bookmarks you create will be kept.

However, you aren't invisible. Going incognito doesn't hide your browsing from your employer, your internet service provider, or the websites you visit.

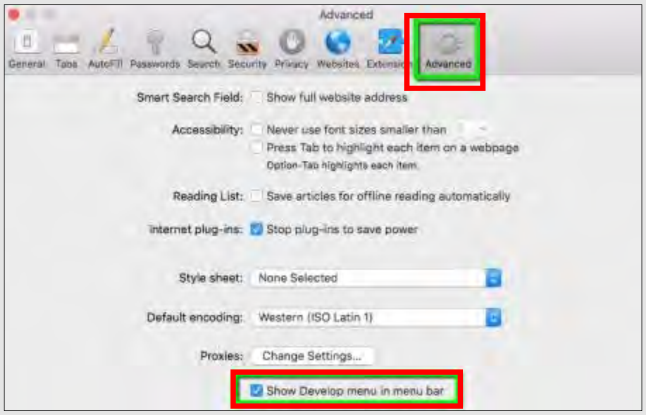
Like Microsoft Edge’s InPrivate Browser, Chrome’s Incognito will require you to constantly type in your password for logins. So you may prefer to use the regular Google Chrome browser out of convenience.

Chrome doesn't have control over third party websites or their privacy practices, so be cautious when accessing websites.

UPDATED JAN 2021

DELETE BROWSER ARTIFACTS SMART CARD

Deleting Safari Browser Artifacts



Smart Search Field: □ Show full website address

Accessibility: □ Never use font sizes smaller than
□ Press Tab to highlight each item on a webpage
Option-Tab highlights each item.

Reading List: □ Save articles for offline reading automatically

Internet plug-ins: ☑ Stop plug-ins to save power

Style sheet: None Selected

Default encoding: Western (ISO Latin 1)

Proxies: Change Settings...

☑ Show Develop menu in menu bar

Click the “Safari” menu on the top left.

Click “Preferences”.

Click the “Advanced” tab.

Check the box at the bottom for “Show Develop menu in menu bar” and close the window.

Click the “Develop” menu at the top and click “ Empty Caches”.

Then click the “History” menu at the top and click “Clear History”.

Right click on the Safari icon in your App tray and select “Quit”.

Mobile Browser

Open your iOS Settings app.

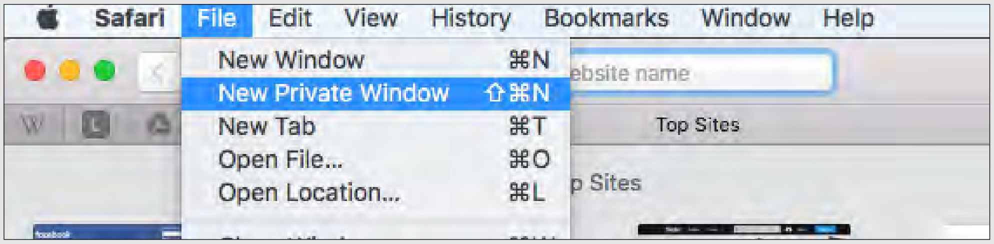
Scroll down and tap “Safari”.

Tap the “Clear History and Website Data” link in blue.

Exit/quit all browser windows and re-open the browser.

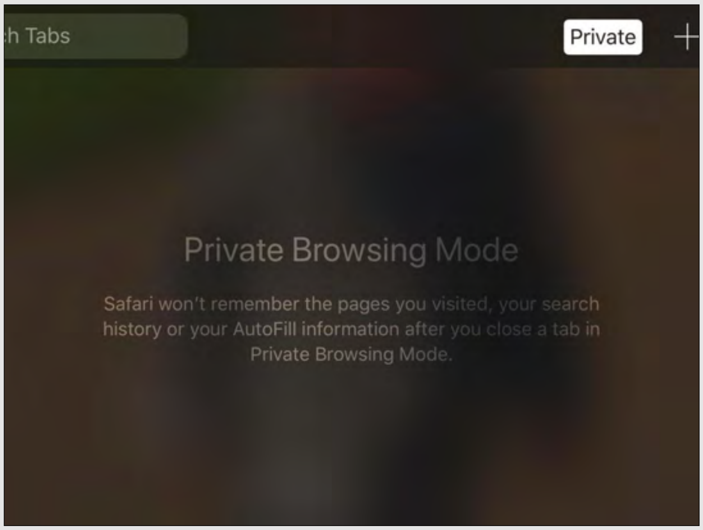
On your Laptop go to “History” in your Safari app, then “Clear History”.

Deleting Safari Browser Artifacts



To open a Private Window, click “File” on the top left.

Click “New Private Window”.



Private Browsing Mode

Safari won't remember the pages you visited, your search history or your AutoFill information after you close a tab in Private Browsing Mode.

Enabling Private Browsing limits Safari in three important ways: It prevents the browser from creating a history of the pages you visit, it stops AutoFill information like website usernames and passwords from being remembered, and any tabs you open won't be stored in iCloud.

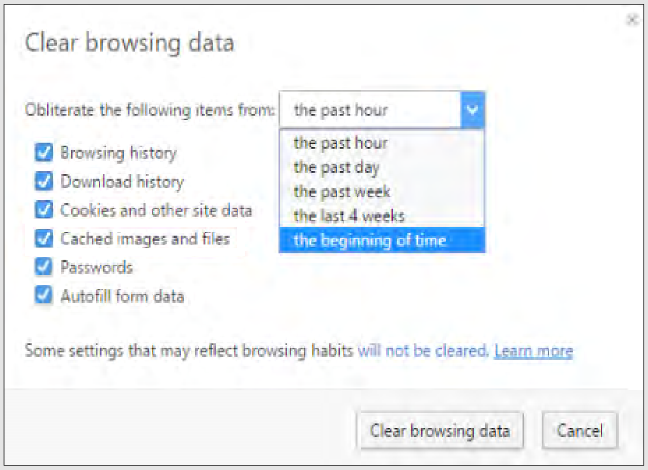
Safari automatically prevents cross-site tracking, and requests that sites and third-party content providers don't track you as a rule. Additionally, the privacy mode stops sites from modifying any information stored on your iOS device, and deletes cookies when you close the associated tab.

When you are on a website that uses Apple Pay, the site can automatically check if you haven't disabled this feature.

UPDATED JAN 2021

DELETE BROWSER ARTIFACTS SMART CARD

Deleting Opera Browser Artifacts



Clear browsing data

Obliterate the following items from: the past hour

- the past hour
- the past day
- the past week
- the last 4 weeks
- the beginning of time

☑ Browsing history
☑ Download history
☑ Cookies and other site data
☑ Cached images and files
☑ Passwords
☑ Autofill form data

Some settings that may reflect browsing habits will not be cleared. Learn more

Clear browsing data | Cancel

Click the "Menu" button on the top left.

Click "History".

Click "Clear Browsing Data".

Select the Time frame and the boxes next to the history you want to remove and click "Clear Browsing Data." Selecting "Advanced" will provide the us-er with more options to clear.

Exit/quit all browser windows and re-open the browser.

Mobile Browser

Tap on the "Menu" button.

Tap "History".

Tap "Clear All".

Tap "Yes" to confirm.

Using a Private Tab in Opera Browser

Opera's Private Tab browsing deletes browsing history, cache, cookies, and logins when you close the tab.

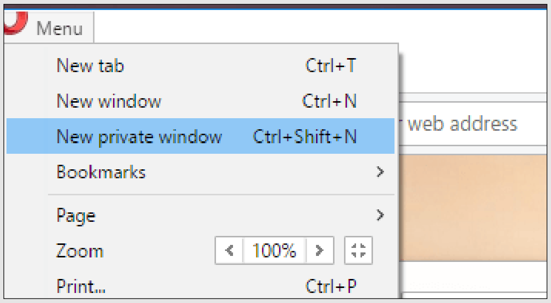
Please note that if you deliberately save data, such as a bookmark or a file, it will still be visible after the tab is closed.

You may prefer to use the regular Opera Browser window out of convenience. Be sure to delete browser artifacts regularly.

To create a Private Tab, click the "Menu" button on the top left corner.

Click "New Private Window".

Private browsing is also available on Opera Mini mobile browser as well.



Menu

New tab	Ctrl+T
New window	Ctrl+N
New private window	Ctrl+Shift+N
Bookmarks	>
Page	>
Zoom	< 100% >
Print...	Ctrl+P

web address

Privacy is about much more than "hiding things". It's about protection. #ProtectYourPrivacy

UPDATED JAN 2021

DELETE BROWSER ARTIFACTS SMART CARD

Privacy and Security-Related Browser Tools

Ghostery is a German-owned freeware browser extension that allows you to choose what to block, on a tracker-by-tracker or site-by-site basis, or a combination of the two.

The tool also offers tracker profiles so you can learn about the companies collecting data on you as you browse the web.

Ghostery looks at the HTML code on each web page you visit to see if there are "tags" or "trackers" placed by a company that works with the website. The tool can determine if the company is showing you ads, collecting data, or giving you added functionality on the page.

The extension is available for Firefox, Chrome, Safari, Internet Explorer, Microsoft Edge, and Opera. It is also accessible via a mobile application for Android, iOS, and Firefox for Android.

AdBlock Plus is a German-based extension that blocks banner ads, pop-up ads, rollover ads, and more. It stops you from visiting known malware-hosting domains and disables third-party tracking cookies and scripts. It can even block video ads on Facebook and YouTube.

This extension works for Android, Chrome, Firefox, Internet Explorer, Opera, Safari, Microsoft Edge and Yandex.

Blur protects your passwords, payments, and privacy from cyber criminals.

The US-based tool masks your passwords, email addresses, credit card numbers, and address information. It also has the ability to create strong passwords for new and existing accounts.

Blur blocks hundreds of companies from collecting your data online and blocks tracking that doesn't rely on cookies.

Free and Premium versions are available. Masked credit card is only available with the Premium version which costs $39/year (Basic), $14.99/month (Unlimited), or $99/year (Unlimited). This extension is available for Chrome, Firefox, Safari, Opera, Internet Explorer, Android, and iOS.

Disconnect is a smart filter that stops third-party sites from tracking you. The companies that are collecting your information are shown in real-time as pages load. You can even see how those sites may be linked to other sites that track information.

Disconnect encrypts the data you exchange with common sites and helps to prevent visiting sites that have malware.

The extension is available for Chrome, Firefox, Safari, and Opera.

Before installing an add-on or extension, review the requested permissions. They may request to access and store to your data.

UPDATED JAN 2021

ADDITIONAL RESOURCES

Free Annual Credit Report
www.annualcreditreport.com

USA.Gov
https://www.usa.gov/identity-theft

Stay Safe Online
www.staysafeonline.org

On Guard Online
www.onguardonline.gov

Equifax—ID Protection Kit
https://www.equifax.com/personal/identity-theft-protection/

Child Identity Theft- Transunion
https://www.transunion.com/fraud-victim-resource/child-identity-theft

Opt Out Prescreen -
https://www.optoutprescreen.com/

Federal Trade Commission—ID Protection Tips
www.consumer.ftc.gov/topics/protecting-your-identity

IRS—ID Protection, Prevention, Detection and Victim Assistance
www.irs.gov/Individuals/Identity-Protection

Netsmartz Workshop for Parent & Guardians
https://www.missingkids.org/NetSmartz

Organization for Social Media Safety
https://www.ofsms.org/

FBI Parents Guide to Internet Safety
www.fbi.gov/stats-services/publications/parent-guide

Kids Games
https://sos.fbi.gov/

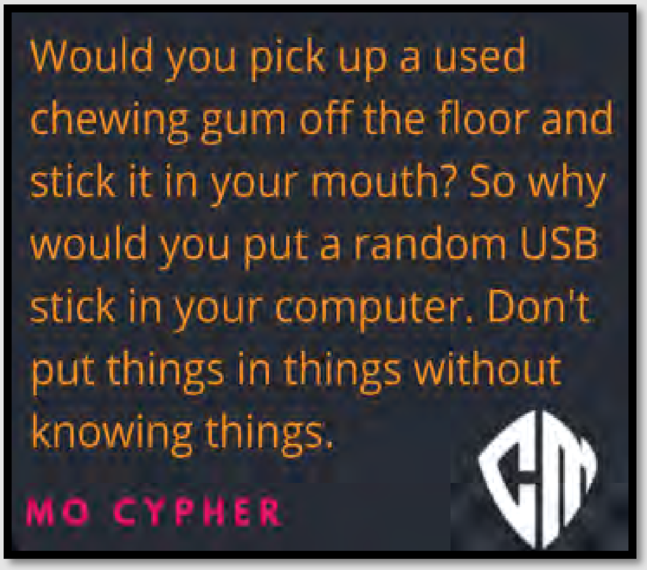
Safety Reviews for Games, Websites, & Apps
www.commonsensemedia.org

Opt Out of Interest-Based Advertising
www.networkadvertising.org/choices

Google Privacy
https://policies.google.com/privacy

DMA Choice
https://dmachoice.thedma.org

Social Media Help (for updated Privacy information)
https://www.facebook.com/help
http://search.twitter.com



Would you pick up a used chewing gum off the floor and stick it in your mouth? So why would you put a random USB stick in your computer. Don't put things in things without knowing things.

MO CYPHER

Remember the more you know the easier it is to prevent something like Identity Theft from happening to you. #stopthinkpost #themoreyouknow