OPERATIONS SECURITY (OPSEC)

THIS PRODUCT WAS PUBLISHED BY NCSC'S ENTERPRISE THREAT-MITIGATION DIRECTORATE & THE NATIONAL OPERATIONS SECURITY PROGRAM (NOP) OFFICE

Protecting Individuals by Practicing OPSEC

National OPSEC Awareness Month, January 2023, Bulletin 3

National Operations Security (OPSEC) Awareness Month provides an opportunity for individuals to assess how they are protecting their personal information and how they can incorporate OPSEC principles into their daily routines to reduce personal risk. The same OPSEC governing principles that are (or should be) applied in the workplace can be integrated into personal lives to protect private information.

There are many ways to incorporate OPSEC principles into daily activities, including placing safeguards on electronic devices and increasing security on social media accounts. Such adjustments make it more difficult for an adversary (i.e., someone with nefarious intent) to obtain information from those devices and accounts.

Device and account factory settings often allow for the most information to be gathered and the least amount of privacy for the user. These settings can be "toggled" to limit the amount of personal data that can be accessed from a cellular device or application. For example, turning off location services can help conceal your location. Setting social media profiles to private and having family members do the same can also help protect private information. Mobile wallets may be convenient to use, but storing financial information on a mobile device also introduces risk. Individuals should closely monitor all online activity and utilize security features such as strong passwords, PINs, and multi-factor authentication to help safeguard personal information.

Employing an OPSEC mindset during daily activities is an important step in protecting private information. Adversaries can compromise commonly used tools and applications, such as emails, texts, direct messaging, and dating apps to gain access to private information. Exercise caution when receiving unsolicited messages (including texts, emails, DMs, chats, etc.), particularly if they come from unknown senders and/or contain suspicious links or attachments. Adding encryption to messages and emails, verifying where and whom a message is coming from, and exercising caution before downloading files and clicking on links are all ways to prevent an adversary from gaining access to private information.

Beyond ways in which private information can be accessed via cyberspace, adversaries may employ other methods to obtain personal information, including:

- Unsolicited phone calls, especially by people pretending to be from the government or an industry you work in
- Intercepting mail or packages that have been delivered and left on your doorstep
- Card skimmers on ATMs or other credit/debit card machines
- Listening to conversations in public spaces where they can overhear your personal information

The same OPSEC strategies and guidelines that are important to protect government and business information are useful in protecting personal information from adversaries. Incorporating OPSEC practices into daily lives is, by definition, good OPSEC.

The National OPSEC Program Office provides OPSEC resources and awareness materials year round. Please visit the following link: National Operations Security Program Office (NOP) (dni.gov)