SPEAR PHISHING AND COMMON CYBER ATTACKS

A spear phishing attack is an attempt to acquire sensitive information or access to a computer system by sending counterfeit messages that appear to be legitimate. “Spear phishing” is a type of phishing campaign that targets a specific person or group and often will include information known to be of interest to the target, such as current events or financial documents. Like other social engineering attacks, spear phishing takes advantage of our most basic human traits, such as a desire to be helpful, provide a positive response to those in authority, a desire to respond positively to someone who shares similar tastes or views, or simple curiosity about contemporary news and events. These messages are delivered via e-mail and are designed to convince the user to open a malicious link or attachment, exposing the target to malicious software.

PHISHING IS NO LONGER AS OBVIOUS AS IT ONCE WAS

The goal of spear phishing is to acquire sensitive information such as usernames, passwords, and other personal information. When a link in a phishing e-mail is opened, it may open a malicious site, which could download unwanted information onto a user’s computer. When the user opens an attachment, malicious software may run which could compromise the security posture of the host. Once a connection is established, the attacker is able to initiate actions that could compromise the integrity of your computer, the network it resides on, and data.

In the past, users could easily detect phishing e-mails, which were often sent from unknown senders, contained misspelled words, and used poor grammar.

Dear User,
Your account expire soon.
Please click here to keep account active.
Sincerely,
The Google Team

Dear Valued Member,

Thank you for trusting us with your banking needs. We have been notified about a phishing email targeting our members, and have attached a notice for your review.

For your protection, please use the link below to verify your account details...

Today, phishing scams are more sophisticated—identities are masked, messages are tailored, and email content appears legitimate. Signs of a phishing scam may include generic greetings, urgent action requests you did not initiate, requests for personal information, and even baseless threats.

Other cyber-attack concerns include compromised or counterfeit websites that introduce malware to obtain a user's Personally Identifiable Information (PII). Skilled hackers can create new websites that appear legitimate or hack into a legitimate site undetected and embed malicious code. Signs of a malicious website include strange or unexpected search engine results and abnormal redirects to unexpected websites. Anti-virus software tools can often catch website redirects and most search engine companies such as Google, Chrome, and Bing alert users to problematic websites and often block access to those with malware.

Here are a few easy things to help protect yourself from phishing and malware cyber-attacks:

- Avoid websites that produce browser alerts and advise against access.
- Do not open email attachments or click links from unknown senders.
- Use a strong password and change it as required.

INTERNET RESOURCES

OnGuardOnline.gov
Operated by the Federal Trade Commission (FTC), this site provides tips and technical guidance on cybersecurity issues as well as a guide for talking to children about Internet use.

StaySafeOnline.org
Offers resources on a variety of cybersecurity issues, including information on adjusting privacy settings on a number of popular platforms.