U.S. ARMY
CYBER COMMAND
www.arcyber.army.mil |

Phishing and Spearphishing

WHAT IS “PHISHING?”

- Email attack is the preferred method for many hackers -- a cybercriminal sends an email that attempts to fraudulently acquire the recipient’s personal information. A phishing email might include an attachment or a link or request personal information. The email may appear to be legitimate communication from your bank, phone company, a store you frequent, or a friend or coworker. A phishing email calls for an action, such as clicking on an embedded link, opening an attachment, or providing personal information.
- Phishing scams work. Verizon’s 2019 Data Breach Investigations Report showed that nearly a third of all data breaches online, and more than three-quarters of cyber-espionage attacks, involved phishing. And it’s getting worse as perpetrators get better and phishing kits that make it easy for cyber criminals to send fraudulent emails and spoof trusted sites or brands become more available.
- Additionally, on some sites that hackers love – social media and banking websites – emails are used as usernames. A hacker who knows his target’s email address would then know their likely username for some accounts and could then try to crack the target’s passwords on those accounts.

WHAT IS “SPEARPHISHING?”

- The higher up you are in an organization, the more likely you are to be a target for spearphishing -- specialized attacks against specific targets or small groups of targets to collect information or gain access to systems. In a spearphishing campaign, hackers have done their homework and learned names of the target’s subordinates, associates, friends, and perhaps even clubs the target belongs to or schools the target’s children attend. Spearphishing emails typically appear to be from or about those close relations. “Whaling” defines attempts to specifically target high-value or senior personnel.

WHAT IS “WHALING?”

- Whaling is similar to spearphishing but specifically targets high-value individuals in an organization. It often uses social engineering and personalized methods to disguise attempts to steal information or money or gain access to systems.

WHAT IS “CLONE PHISHING?”

- Clone phishing is an attack that uses copies and modifications of legitimate existing email to spread malicious links intended to fool the recipient into downloading malware, providing access to systems, sharing sensitive information or visiting fake sites. The cloned emails may look nearly identical to the originals, but with the original attachments or links replaced by malicious ones.

WHAT ARE SOME WAYS TO IDENTIFY PHISHING EMAILS?

- **Poor spelling and grammar.** Cyber criminals normally do not have the staff of copy editors that professional companies or organizations have, so phishing attempts often contain spelling and grammar mistakes.

- **Threats.** Have you ever received a threat that your account would be closed if you didn't respond to an email message? Cybercriminals often use threats that your security has been compromised.
- **Spoofing popular websites or companies.** Scam artists use graphics that appear to be connected to legitimate websites, but take you to scam sites or legitimate-looking pop-up windows. Cybercriminals also use web addresses that resemble the names of well-known companies but are slightly altered.

WHAT ARE SOME WAYS TO IDENTIFY CLONED EMAILS?

- **Bogus or broken links.** Links to non-professional or unknown websites, or broken image links due to copy-paste errors.
- **Mystery attachments.** Attachments to an email that originally had no attachments.
- **Suspicious addresses.** Email addresses that don't match the addess of the original sender.
- **Poor added content.** Text added to the original email content, but with typos or bad grammar.

WHAT CAN I DO TO HELP AVOID BECOMING A VICTIM OF PHISHING AND SPEARPHISHING?

- **Beware of links in email.** Rest your mouse on the link (but don't click!) to see if the address matches the link typed in the message. The real address should show in a small box. If it doesn't look anything like the link text or the company's web address, it's best not to click on it.
- **Call before you click.** Suppose you have an email that seems to be from your organization's human resources department telling you to complete an attached form to "update your personnel file." The attachment could be an executable malware file or it could be a legitimate personnel update. Fight the natural instinct to trust an official-looking communication. Assume it's malware until proven otherwise.
- **When in doubt, throw it out.** If it looks suspicious, even if you know the source, it's best to delete it or, if appropriate, mark it as junk email.
- **Consider using specialized email accounts.** Use one account for work, one for friends, and one for online purchases. If you create a unique email address just for online payments, for example, it will be harder for a hacker to gain access to your information and account.
- **If you are a victim of phishing, report it.** Report phishing attempts to the appropriate experts within your organization, such as network administrators and security officers. If you believe your financial accounts may be compromised, contact your financial institutions immediately. Additionally, consider reporting the attack to your local police department, and file a report with the Federal Trade Commission, the Anti-Phishing Working Group (APWG), and/or the FBI's Internet Crime Complaint Center.

WHAT ABOUT PHISHING PHONE CALLS?

- Email isn't the only way criminals launch phishing attempts. They might also attempt to scam you by phone, claiming to represent a trusted firm. Once they gain your trust, they may ask you for your user name and password or direct you to a website to install software that allows them to access your computer. Be wary of unsolicited calls and report them to your security manager and/or other appropriate authority.
- Callback phishing combines email and phone calls. Callback phishing starts with a phishing email that directs you to call a number instead of clicking on a link in the email. When the number is called, the cybercriminal will try to trick the unsuspecting victim into providing sensitive information. Another version involves crooks sending an email claiming that the victim has a pending charge on an account, and directing them to a help number. When the number is called the victim is guided through steps that allow the scammer to install ransomware that can be used to steal information or extort the caller. To help avoid becoming a victim, be wary of emails that contain a sense of emergency to try to get you to act impulsively, consider the details of the email (would your bank normally ask you to call them?), and don't call numbers provided in emails -- if you have questions, find a trusted number independently.