ONLINE SAFETY BASICS

Spam and Phishing

Cybercriminals have become quite savvy in their attempts to lure people in and get you to click on a link or open an attachment.

Malicious Email - A malicious email can look just like it comes from a financial institution, an e-commerce site, a government agency or any other service or business. It often urges you to act quickly, because your account has been compromised, your order cannot be fulfilled or there is another urgent matter to address. If you are unsure whether an email request is legitimate, try to verify it with these steps:

- Contact the company directly – using information provided on an account statement, on the company's official website or on the back of a credit card.
- Search for the company online – but not with information provided in the email.

Spam - Spam is the electronic equivalent of junk mail. The term refers to unsolicited, bulk – and often unwanted – email. Here are ways to reduce spam:

- **Enable filters on your email programs:** Most internet service providers (ISPs) and email providers offer spam filters; however, depending on the level you set, you may end up blocking emails you want. It's a good idea to occasionally check your junk folder to ensure the filters are working properly.
- **Report spam:** Most email clients offer ways to mark an email as spam or report instances of spam. Reporting spam will also help to prevent the messages from being directly delivered to your inbox.
- **Own your online presence:** Consider hiding your email address from online profiles and social networking sites or only allowing certain people to view your personal information.

Phishing - Phishing attacks use email or malicious websites (clicking on a link) to collect personal and financial information or infect your machine with malware and viruses.

Spear Phishing - Spear phishing involves highly specialized attacks against specific targets or small groups of targets to collect information or gain access to systems. For example, a cybercriminal may launch a spear phishing attack against a business to gain credentials to access a list of customers. From that attack, they may launch a phishing attack against the customers of the business. Since they have gained access to the network, the email they send may look even more authentic and because the recipient is already customer of the business, the email may more easily make it through filters and the recipient maybe more likely to open the email.

The cybercriminal can use even more devious social engineering efforts such as indicating there is an important technical update or new lower pricing to lure people.

Spam & Phishing on Social Networks - Spam, phishing and other scams aren't limited to just email. They're also prevalent on social networking sites. The same rules apply on social networks: When in doubt, throw it out. This rule applies to links in online ads, status updates, tweets and other posts. Here are ways to report spam and phishing on major social networks:

- **Facebook** - https://www.facebook.com/help/217854714899185
- **Twitter** – https://help.twitter.com/en/safety-and-security/report-spam
- **Youtube** - https://support.google.com/youtube/answer/2801973?hl=en

Tips for Avoiding Being a Victim

Compliments of…

WSC WISCUB
Service Center

- **Don't reveal personal or financial information in an email**, and do not respond to email solicitations for this information. This includes following links sent in email.
- Before sending or entering sensitive information online, **check the security of the website**.
- **Pay attention to the website's URL.** Malicious websites may look identical to a legitimate site, but the URL may use a variation in spelling or a different domain (e.g., .com versus .net).
- If you are unsure whether an email request is legitimate, **try to verify it by contacting the company directly**. Contact the company using information provided on an account statement, not information provided in an email.
- **Keep a clean machine.** Keep all software on internet-connected devices – including PCs, smartphones and tablets – up to date to reduce risk of infection from malware.

What to Do if You Are a Victim

- **Report it to the appropriate people** within the organization, including network administrators. They can be alert for any suspicious or unusual activity.
- If you believe your financial accounts may be compromised, **contact your financial institution immediately** and close the account(s).
- **Watch for any unauthorized charges** to your account.
- **Consider reporting the attack** to your local police department, and file a report with the Federal Trade Commission or the Internet Crime Complaint Center.
- Protect Yourself With These STOP. THINK. CONNECT.™ Tips
- **When in doubt, throw it out:** Links in email, tweets, posts and online advertising are often how cybercriminals try to compromise your information. If it looks suspicious, even if you know the source, it's best to delete or – if appropriate – mark it as junk.
- **Think before you act:** Be wary of communications that implores you to act immediately, offers something that sounds too good to be true or asks for personal information.
- **Make your password a sentence**: A strong password is a sentence that is at least 12 characters long. Focus on positive sentences or phrases that you like to think about and are easy to remember (for example, "I love country music."). On many sites, you can even use spaces!
- **Unique account, unique password:** Having separate passwords for every account helps to thwart cybercriminals. At a minimum, separate your work and personal accounts and make sure that your critical accounts have the strongest passwords.
- **Lock down your login:** Fortify your online accounts by enabling the strongest authentication tools available, such as biometrics, security keys or a unique one-time code through an app on your mobile device. Your usernames and passwords are not enough to protect key accounts like email, banking and social media.

Additional Resources

- Anti-Phishing Working Group - https://www.us-cert.gov/ncas/tips/ST04-014
- OnGuardOnline - https://www.consumer.ftc.gov/features/feature-0038-onguardonline
- United States Computer Emergency Readiness Team (US-CERT) - https://www.us-cert.gov/ncas/tips/ST04-014

Find more information at https://www.staysafeonline.org

Compliments of…

WSC WISCUB
Service Center