Cybersecurity Awareness Month wrap-up

By Information Technology

Our chance to recognize cybersecurity awareness one month of the year is always a reminder to make choices every day to keep cyber threats at bay! Thank you for joining us during the month of October, learning how to Do Your Part #BeCyberSmart. Here are the key takeaways:

Never send money via gift card or wire transfer to someone you have never met face-to-face. Seriously, just don't do it. If they ask you to use wire transfer, a prepaid debit card, or a gift card, those cannot be traced and are as good as cash. Chances are, you won't see your money again.

Don't take calls from unknown numbers. Your phone is one of the most common and easiest ways for a scam to sneak into your life. Caller ID is no longer reliable; scammers "spoof" recognized numbers to fool you into answering. A common one being tech support scams where callers, supposedly from Microsoft or ISPs (internet service providers) try to gain access to your computer. Your best bet: unless you recognize and are expecting a call from a number, let the call go to voice mail. You can then determine what action to take if any.

Create passwords with at least 15 characters. The longer a password is the better. Each account should have a different password and when offered, utilize multi-factor authentication. Keep passwords safely stored in one stop with a password manager, such as LastPass.

Slow down and determine if legitimate. Scammers are great at mimicking email addresses, logos and other details. Just because a website or email looks official does not mean that it is as shown in examples we received last month.

Refrain from clicking on links or open attachments in unsolicited email messages. Links can download malware onto your computer that steal your identity or try to capture information like passwords. Be cautious even with emails that look familiar; it could be fake.

Only share appropriate information. Never share your personal information or financial information to anyone over the phone, email, or social media unless you solicit the call yourself. This includes passwords, banking and credit card information, your birthdate and Social Security numbers.

Protecting your mobile phone and managing scam calls. Your phone is as powerful as your computer, which is even more reason to keep it secure, up to date and safely connected. Call filtering apps available thru providers (AT&T, Verizon, etc.) can also help you with unsolicited callers, identifying callers as "potential spam" or even block some known spam callers after one ring.

Your network devices, such as your router serve an important function. They connect you to everything online. It is important they are up to date and secured, including your Wi-Fi network.

Thanks again for joining us. Each one of us can play a part to make sure that our online lives are kept safe and secure. If you would like to learn more, you can visit the official NCSAM site. If you have any questions or feedback, please reach out to us at 1-800-373-7521 or helpdesk@ssndcp.org.

Take the time to question the validity of any interaction, whether it be a phone call, email, text message or alert that pops up on the computer. As cyber-attacks are always on the rise and as the world evolves so do the scams, giving us more reason to be ever cautious.