National Cybersecurity Awareness Month

October 30, 2019

Did you know this month is National Cybersecurity Awareness Month?

National Cybersecurity Awareness Month (NCSAM) is a collaborative effort between government and industry to raise awareness about the importance of cybersecurity and to ensure that all Americans have the resources they need to be safer and more secure online. NCSAM 2019 emphasizes personal accountability and stresses the importance of taking proactive steps to enhance cybersecurity at home and in the workplace. This year's overarching message – Own IT. Secure IT. Protect IT. –focuses on key areas including citizen privacy, consumer devices, and e-commerce security.

Of course, we believe every month should be focused on Cybersecurity Awareness. Here are Top Tips from NCSAM:

- **Double your login protection.** Enable multi-factor authentication (MFA) to ensure that the only person who has access to your account is you. Use it for email, banking, social media, and any other service that requires logging in. If MFA is an option, enable it by using a trusted mobile device, such as your smartphone, an authenticator app, or a secure token—a small physical device that can hook onto your key ring. Read the Multi-Factor Authentication (MFA) How-to-Guide for more information.

- **Shake up your password protocol.** According to National Institute for Standards and Technology (NIST) guidance, you should consider using the longest password or passphrase permissible. Get creative and customize your standard password for different sites, which can prevent cybercriminals from gaining access to these accounts and protect you in the event of a breach. Use password managers to generate and remember different, complex passwords for each of your accounts. Read the Creating a Password Tip Sheet for more information.

- **If you connect, you must protect**. Whether it's your computer, smartphone, game device, or other network devices, the best defense against viruses and malware is to update to the latest security software, web browser, and operating systems. Sign up for automatic updates, if you can, and protect your devices with antivirus software. Read the Phishing Tip Sheet for more information.

- **Play hard to get with strangers.** Cybercriminals use phishing tactics, hoping to fool their victims. If you're unsure who an email is from—even if the details appear accurate— or if the email looks "phishy," do not respond and do not click on any links or attachments found in that email. When available use the "junk" or "block" option to no longer receive messages from a particular sender.

- **Never click and tell**. Limit what information you post on social media—from personal addresses to where you like to grab coffee. What many people don't realize is that these seemingly random details are all criminals need to know to target you, your loved ones, and your physical belongings—online and in the physical world. Keep Social Security numbers, account numbers, and passwords private, as well as specific information about yourself, such as your full name, address, birthday, and even vacation plans. Disable location services that allow anyone to see where you are – and where you aren't – at any given time. Read the Social Media Cybersecurity Tip Sheet for more information.

- **Keep tabs on your apps**. Most connected appliances, toys, and devices are supported by a mobile application. Your mobile device could be filled with suspicious apps running in the background or using default permissions you never realized you approved—gathering your personal information without your knowledge while also putting your identity and privacy at risk. Check your app permissions and use the "rule of least privilege" to delete what you don't need or no longer use. Learn to just say "no" to privilege requests that don't make sense. Only download apps from trusted vendors and sources.

- **Stay protected while connected.** Before you connect to any public wireless hotspot – like at an airport, hotel, or café – be sure to confirm the name of the network and exact login procedures with appropriate staff to ensure that the network is legitimate. If you do use an unsecured public access point, practice good Internet hygiene by avoiding sensitive activities (e.g., banking) that require passwords or credit cards. Your personal hotspot is often a safer alternative to free Wi-Fi. Only use sites that begin with "https://" when online shopping or banking.

To learn more, visit the National Cybersecurity Awareness Month website.