Cyber Savvy password tips for Cybersecurity Awareness Month 2022

Stephen Robison | Monday, October 10, 2022

What is Cybersecurity Awareness Month?

Every year since 2004, the president and congress have declared October as Cybersecurity Awareness Month. The initiative has helped individuals protect themselves as cyber threats that compromise technology, businesses, and personal information have become commonplace. This year, the Cybersecurity & Infrastructure Security Agency (CISA) stated the theme for 2022 – See Yourself in Cyber – is meant to "demonstrate that everyone is responsible for their own online behavior."

Commonly Used Cyber Terms

- **Unauthorized access:** When a person gains entry to a computer network, systems, application software, data, or other resources without permission. Any access to an information system or network that violates the owner or operator's stated security policy is considered unauthorized access.
- **Exfiltration:** The theft or unauthorized removal or movement of any data from a device.
- **Threat actor:** Any individual conducting cybercrimes; including but not limited to hackers, social engineers, shoulder surfers, and ransomware groups.
- **Hackers:** Use computers and other digital devices to gain unauthorized access to information or damage computer systems. Hackers may have impressive computer skills, but expert knowledge of programming is not always necessary for a successful breach. Any attempt by threat actors or hackers to gain unauthorized access to a digital computer system can constitute a cybercrime.

What is considered a cybercrime and attack?

Cybercrime has been defined as any crime that is committed electronically. The crimes include fraud, theft, ransom, and even physical attacks on a system. While most of the incidents happen through an external force, such as a phishing email or dangerous link, they can also occur through the use of storage devices such as a USB, flash drives, or even connecting local devices to the same environment. Overall, these actions lead to the abuse and exploitation of vulnerabilities within a system for the criminal to capitalize on and extort.

Why you should care and password tips

Like your home and car, you should not leave you digital systems and data vulnerable to an attack. Your data and computer system should be "locked" and handled with the same care as your other belongings. Any device that stores information or is connected to the internet can be a way for cyber criminals to gain access to your information and personal data. Your password is one of the first lines of defense. Listed below are password tips provided by CISA:

- **Use different passwords on different accounts.** One of the leading causes of unauthorized access to accounts is the reuse of login credentials.
- **Use the longest password allowed.** The longer and more complicated a password is, the harder it will be for someone to access your accounts. Use 11 characters or more, a short sentence or a mix of letters, symbols and numbers to strengthen your passwords.
- **Reset your password every few months.** Reset your passwords regularly, especially when these passwords allow access to confidential accounts, such as banking or medical data. It is vital to reset passwords as it takes most companies an average of six months to notice that a data breach has happened. By the time a data breach is reported, a threat actor could already be using and/or selling your data.
- **Use a password manager.** With just one master password, a password manager can generate and retrieve passwords for every account that you have – encrypting and protecting your online information, including credit card numbers and their three-digit Card Verification Value (CVV) codes, answers to security questions and more.

While a strong password is a great start, McDonald Hopkins' national Data Privacy and Cybersecurity Practice Group can help you find more ways to protect your business and your personal data. Keep an eye out this month as McDonald Hopkins continues to publish helpful tips and strategies you and your business can use to "See Yourself in Cyber."

Stephen Robison