October, 2019
Volume 14, Issue 10

Own IT. – Secure IT. – Protect IT.

From the desk of Thomas F. Duffy, MS-ISAC Chair

The 16th annual National Cybersecurity Awareness Month (NCSAM) is in full swing! Held every October, NCSAM has been a collaborative effort between government and industry to raise awareness about not only the importance of cybersecurity, but also ensure that everyone has access to the appropriate resources they need to be safer and more secure online.

Since NCSAM's inception (under the leadership of the U.S. Department of Homeland Security and the National Cyber Security Alliance, or NCSA), it has vastly accelerated, reaching a multitude of consumers, both small and medium-sized businesses, corporations, educational institutions and an exponential amount of young people across the country.

Following the success of the 'Our Shared Responsibility' theme last year, CISA and NCSA have now shifted towards a more personalized approach, gearing their message towards individual accountability. This year's overarching message – *Own IT. Secure IT. Protect IT.* – has been designed to not only encourage personal accountability and proactive behavior in digital privacy, but also promote security best practices, consumer device privacy, e-commerce security, as well as various cybersecurity focused careers. Below are some of the highlighted calls to action and their key messages:

Own IT.

We live in a world in which we are constantly connected, so cybersecurity cannot be limited to the home or office. When you're traveling, it is always important to practice safe online behavior and take proactive steps to secure your smart devices. With every social media account you sign up for, every picture you post, and status you update, you are sharing information about yourself with the world.

- **Double your login protection.** Enable multi-factor authentication (MFA) to ensure that the only person who has access to your account is you.
- **Update your privacy settings:** Set the privacy and security settings to your comfort level for information sharing. Keep tabs on your apps and disable geotagging (which allows anyone to see where you are).
- **Connect only with people you trust:** While some social networks might seem safer, always keep your connections to people you know and trust.

Secure IT.

Have you noticed how often security breaches, stolen data, and even identity theft, are front-page headlines nowadays? Cybercriminals attempt to lure users to click on a link or open an attachment that may infect their computers. These emails might also request personal information such as bank account numbers, passwords, or Social Security numbers. When users respond with the information or click on a link, these attackers now possess access to their personal accounts.

- **Avoid using common words in your password:** Substitute letters with numbers and punctuation marks or symbols. For example, @ can replace the letter "A"/
- **Be up to date:** Keep your software updated to the latest version available. Turn on automatic updates so you don't have to think about it!
- **Think before you act:** Be wary of communications which implore you to act fast. Many phishing emails create urgency, instilling fear that your account or information is in jeopardy.

Protect IT.

Today's technology allows us to connect around the world through banking, shopping, streaming, and more. This added convenience undoubtedly comes with an increased risk of identity theft and scams. More and more home devices (such as thermostats, door locks, etc.) are now connected. While this may save us time and money, it poses new security risks.

- **Secure your Wi-Fi network:** Your home's wireless router is the primary entrance for cybercriminals to access all of your connected devices, and you can better secure your Wi-Fi network and devices by changing the factory-set default password and username for each one.
- **Know what to look for:**
  - **Identity Theft** – bills for products or services you did not purchase, suspicious charges on your credit cards, or any changes to your accounts that you did not authorize.
  - **Imposter Scams** – an imposter may contact you saying they are from a trusted organization informing you that your SSN has been suspended, or your account has been locked, while asking for your sensitive information or payment to fix the issue.
  - **Debt Collection Scams** – scammers may attempt to collect on a fraudulent debt. Debt collector scammers typically request payment by wire transfers, credit cards, or gift cards.

Visit these sites to learn more:
https://niccs.us-cert.gov/national-cybersecurity-awareness-month-2019
https://staysafeonline.org/ncsam/about-ncsam/

MS-ISAC
Multi-State Information Sharing & Analysis Center

STOP | THINK CONNECT™