October, 2017
Volume 12, Issue 10

National Cyber Security Awareness Month

The Internet is a shared resource, and securing it is our shared responsibility.

OhioDAS
SERVICE · SUPPORT · SOLUTIONS
DEPARTMENT OF ADMINISTRATIVE SERVICES

Office of Information Security and Privacy

From the desk of Russ Forsythe, Chief Information Security Officer

National Cyber Security Awareness Month (NCSAM) is now its 14th year. This annual month-long event dedicates October to reminding all digital citizens and businesses that protecting our computers and networks is "Our Shared Responsibility" and that everyone plays a critical role in promoting safe computing. The NCSAM is led by the National Cyber Security Alliance (NCSA) and the U.S. Department of Homeland Security (DHS). The month's primary goal is to provide Internet users and businesses with the information and tools they need to be safer and more secure online, including education about how to protect personal information in today's highly connected world. Everyone can join in and be a part of the something big by becoming a NCSAM 2017 Champion. Hundreds of organizations and individuals have officially signed on as Champions to support the month. NCSAM Champions strengthen and boost the greater effort by spreading the word and host NCSAM Partner Events about online safety at home, at work, and in the community.

NCSAM 2017 kicked off on October 1st with a strong reminder for all digital citizens to

STOP: make sure security measures are in place
THINK: about the consequences of your actions and behaviors online
CONNECT: and enjoy the Internet.

Our second week's theme was:

Cybersecurity in the Workplace is Everyone's Business

Whatever your place of work – whether it's a large or small organization, healthcare provider, academic institution or government agency – creating a culture of cybersecurity from the breakroom to the board room is essential and a shared responsibility among all employees. NCSA's advice, based on national standards, recommends that organizations have a plan in place to **identify** your digital "crown jewels," **protect** your assets, be able to **detect** incidents, have a plan for **responding**, and quickly **recover** normal operations. You can help your organization do this: take part in cybersecurity discussions, learn how to protect the digital "crown jewels," and what to do if you detect an incident. Then expand this to your home: identify what you would hate to lose, and ensure that information is protected with antivirus software

and backed up somewhere else. Be sure everyone in your family knows how to detect and recover from an incident.
NCSA and DHS are highlighting particular themes as we continue through the month. We invite you to join in each coming week, with the following user-friendly, actionable advice:

Week 3: Oct. 16-20 ***Today's Predictions for Tomorrow's Internet***
Take a look into our future through the lens of the connected Internet and identify strategies for security, safety, and privacy while leveraging the latest technology. With the explosion of digital interconnectivity, it is critical to explore everyone's role in protecting our cyber ecosystem. NCSA's top tips include:

- **Learn how to safeguard your Internet of Things (IoT) devices**: Protecting devices like wearables and smart appliances can be different than securing your computer or smartphone. Research how to keep an IoT device secure before you purchase it and take steps to safeguard your device over time.
- **Pay attention to the Wi-Fi router in your home**: Use a strong password to protect the device, keep it up-to-date and name it in a way that won't let people know it belongs to you.
- **Delete when done**: Many of us download apps for specific purposes or have apps that are no longer useful or interesting to us. It's a good security practice to delete apps you no longer use.

Week 4: Oct. 23-27 ***The Internet Wants You: Consider a Career in Cybersecurity***
A key risk to our economy and security is the shortage of cybersecurity professionals to protect our extensive networks. Growing the next generation of a skilled cybersecurity workforce – along with training those already in the workforce – is a starting point to building stronger defenses. Here are a couple of to-dos for parents or anyone interested in a cybersecurity career of their own:

- Volunteer at schools, after-school programs, boys and girls clubs, and community workshops to teach kids about online safety and cybersecurity careers. Check out NCSA's online safety resources for ideas on what to cover and materials you can use.
- Learn more about starting your own path to a cybersecurity career by checking out the National Initiative for Cybersecurity Education (NICE) Framework. The framework provides information on what knowledge, skills, and abilities are valued by employers for different cybersecurity jobs.

Visit these sites to learn more:

StaySafeOnline.org/NCSAM DHS.gov/NCSAM StopThinkConnect.org

MS-ISAC
Multi-State Information Sharing & Analysis Center

STOP | THINK CONNECT™