October, 2018
Volume 13, Issue 10

October – National Cybersecurity Awareness Month

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

The 15th annual National Cybersecurity Awareness Month (NCSAM) is almost here! October 1st will kick off this month-long campaign devoted to ensuring everyone has the resources they need to stay safe online. NCSAM is co-led by the National Cyber Security Alliance (NCSA) and the U.S. Department of Homeland Security, and is championed by the Multi-State Information Sharing and Analysis Center (MS-ISAC). NCSA encourages everyone to support NCSAM by signing on as Champions. It's free to join and Champions receive weekly emails with user-friendly infographics, memes, and sample social media posts to stay involved.

Each week of October highlights a theme that contributes to that "Shared Responsibility" of online safety and security. In partnership with NCSA, below we have provided some tips for how to make the most of those themes and strengthen our individual and national cybersecurity!

Week 1: Make Your Home a Haven for Online Safety

Easy-to-learn life lessons for online safety and privacy begin with parents and caregivers leading the way. Family members may be using the Internet to engage in social media, adjust the home thermostat, or to shop for the latest connected toy. This makes it vital to ensure that the entire household – including children – learn to use the Internet safely and responsibly, and that networks and mobile devices are secure. Three of NCSA's top tips include the following:

- **Keep a clean machine**: Keep all software on Internet-connected devices, including personal computers, smartphones and tablets, up-to-date to reduce risk of infection from ransomware and malware.
- **Lock down your login:** Your usernames and passwords are not enough to protect key accounts like email, banking, and social media. Fortify your online accounts and enable the strongest authentication tools available, such as biometrics, or two-factor authentication.
- **Share the best of yourself online**: Before posting online, think about what others might learn about you and who might see it in the future, such as teachers, parents, colleges, and potential employers.

Week 2: Millions of Rewarding Jobs: Educating for a Career in Cybersecurity

A key risk to our economy and security continues to be the shortage of cybersecurity professionals to safeguard our ever-expanding cyber ecosystem. There are limitless opportunities for students and individuals looking for a new career or re-entering the workforce. Here are some tried and true tips for cyber job seekers at any age:

- **Get Credentialed:** Four out of five cybersecurity jobs require a college degree. Certifications can also be valuable to display your specialized knowledge. DHS offers free online, on-demand courses

through the Federal Virtual Training Environment that provide great learning opportunities for public employees and veterans.
- **Get Involved**: Test the waters through volunteer work and internships. Offer to help technical professionals at your school or workplace to gain experience. You could even consider joining local clubs or groups, such as those on MeetUp. (Remember to be safe when meeting people or going to new places!)
- **Keep Up with the Buzz**: Follow top cybersecurity personalities on Facebook, Twitter, LinkedIn, and news websites and blogs.

Week 3: It's Everyone's Job to Ensure Online Safety at Work

When you are on the job, your organization's online safety and security is also part of your responsibility. NCSA's CyberSecure My Business™ will be a cornerstone for Week 3. The program is a series of in-person and highly interactive workshops based on the NIST Cybersecurity Framework to educate the community about:
- understanding which business assets ("digital crown jewels") others want;
- learning how to protect those assets;
- detecting when something has gone wrong;
- reacting quickly to minimize impact and implement an action plan; and
- learning what resources are needed to recover after a breach.

Additional components include monthly webinars, online portal resources, and monthly newsletters summarizing the latest cybersecurity news. NCSA has also created a Cybersecurity Awareness Toolkit, which is packed with easy-to-use tips and practical information.

Week 4: Safeguarding the Nation's Critical Infrastructure

Our daily lives depend on 16 critical infrastructure sectors, which supply food, water, financial services, public health, government services, communications, transportation, and power along with other critical functionality. A disruption to this system, most of which is operated via the Internet, can result in significant and even catastrophic consequences. Week 4 will highlight the roles the public can play in keeping it safe. Two easy tips everyone should practice to help protect the country's critical infrastructure are:
- **When in doubt, throw it out:** Links in email, tweets, posts and online advertising are often how cybercriminals try to compromise your information. If it looks suspicious, it's best to delete it.
- **Safer for me, more secure for all:** What you do online affects everyone. Good online habits help the nation's digital community.

Visit these sites to learn more:

StaySafeOnline DHS and NCSAM StopThinkConnect

MS-ISAC Multi-State Information Sharing & Analysis Center

NATIONAL CYBERSECURITY ALLIANCE