

Information Security Newsletter

October 2018



National Cybersecurity
Awareness Month

From the Desk of Milind Samant, ISO

The month of October is the National Cybersecurity Awareness Month (NCSAM). NCSAM is co-led by the National Cyber Security Alliance (NCSA) and the U.S. Department of Homeland Security. SUNY OW supports NCSAM and has signed on as Champions to stay involved with the NCSA activities.

Each of the following four themes contributes towards the “Shared Responsibility” of online safety and security. In partnership with NCSA, ITS is providing some tips on how to make the most of these themes and strengthen individual, institutional and national cybersecurity!

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.

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. Please share the following true tips with anyone you know who is a cyber job seeker:

- **Get Credentialed:** Four out of five cybersecurity jobs require a college degree. Certifications can also be valuable to display your specialized knowledge.
- **Get Involved:** Job seekers can test the waters through volunteer work and internships. ITS can offer help to technical professionals to gain work experience through our internship program.
- **Keep Up with the Buzz:** Follow top cybersecurity personalities on Facebook, Twitter, LinkedIn, and news websites and blogs.

It's Everyone's Job to Ensure Online Safety at Work

When you are on the job, SUNY OW's online safety and security is also part of your responsibility. NCSA utilizes NIST Cybersecurity Framework to educate the community about:

- learning how to protect the institution's digital assets;
- detecting when something has gone wrong;
- reacting quickly to minimize impact and implement an action plan; and

NCSA has also created a Cybersecurity Awareness Toolkit, which is packed with easy-to-use tips and practical information and is available at: <https://staysafeonline.org/resource/cybersecurity-awareness-toolkit/>

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. The fourth theme 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.

Reminders....

- **Set a strong password:** Use at least 8 characters in upper and lower case, numbers, and symbols.
- **Keep your device locked:** Use a password, pin, pattern, or fingerprint lock when you are not actively using it.
- **When in doubt, throw it out and contact the Service Desk at servicedesk@oldwestbury.edu or call X3098.**

Provided By:

<p>Information Technology Services Division of Business & Finance Evan Kobolakis, CIO Len Davis, Sr. Vice President & CFO</p>	 <p>NATIONAL CYBERSECURITY ALLIANCE</p>	 <p>SUNY OLD WESTBURY OWN YOUR FUTURE</p>
---	--	--

The information provided in the Monthly Information Security Newsletter is intended to increase the data security awareness of SUNY Old Westbury end users and to help them behave in a more secure manner within SUNY Old Westbury work environment. While some of the tips may relate to maintaining a home computer, the increased awareness is intended to help improve the SUNY Old Westbury's overall cyber security posture.

Disclaimer: These links are provided because they have information that may be useful. The SUNY Old Westbury ITS Department does not warrant the accuracy of any information contained in the links and neither endorses nor intends to promote the advertising of the resources listed herein.