Information Security Newsletter

March 2017

ITS INFORMATION SECURITY
SUNY OLD WESTBURY

Common IT Wisdom That

Keeps You Secure !

From the Desk of Milind Samant, ISO

Day in and day out, SUNY OW employees hear the same things from ITS staff about cybersecurity and safety. Though often they may sound like a broken record, there are very important reasons and rationale behind these practices and advice. Keeping safe and secure while connected isn't just about how our system is set up - it is also very much about how SUNY Old Westbury employees end up using it. Below, I am discussing some common ITS staff wisdom and trying to provide some background information and the rationale as to why it definitely merits your attention.

Make sure you lock your screen when you are away from your desk.

Screen locking policies exist for a reason. Even if you are leaving for just a few minutes at a time, be sure to lock your screen. Though physical intruders are rare during daytime and in conventionally secured offices, intrusions do occasionally happen. Screen locks also thwart opportunistic insider attacks from other employees that may seek to obtain information or access information beyond what they should normally have. If you don't adhere to a screen locking policy, an attacker can simply walk up and start manipulating or stealing information without having to even work at getting in to our system. And remember, you are ultimately responsible for everything done under your login!

Don't write down your passwords or user credentials.

The same concept applies here as in establishing a screen lock on your system. On the rare occasion a physical attacker gains access to your desk area, they will immediately look for written passwords and authentication material. Post-it notes, index cards, etc. aren't secure from attackers even if you think they might be out of sight under your keyboard! From looking at your written password, they can get right into your sensitive protected office systems and start stealing University's data or compromising digital assets. This risk isn't only from a completely unknown outsider, but could be coming from contractors or internal staff with malicious intent.

Don't re-use your office computer password for other systems and services.

One of the most risky things a person can do is use the same password across multiple accounts or systems. Cyber threat actors are constantly stealing login credentials from numerous systems that may be more insecure, like online shopping sites for example. Many times, these credentials are leaked online for other cyber criminals to also exploit. They then are able to take these stolen credentials and use them to try to access more secure systems, like online banking, or your office systems. If you unfortunately follow this practice of re-using your work password elsewhere, you leave yourself and your organization open to this type of compromise.

Don't install unauthorized software on any office systems.

The installation of unauthorized software can negatively affect the overall information security posture for SUNY Old Westbury. This software can include everything from stand-alone programs to plug-ins for the web browser. Not only can this pose a stability issue leading to slower or unreliable system performance, but the installation of unmanaged software can pose a direct security threat either because it may be malicious software itself, or because this is introducing software that is not part of the patch management system in our environment. If this new unauthorized software ends up making you vulnerable to cyber-attacks in the future, but ITS isn't aware of it or implementing regular patches or fixes, you leave that avenue open for attackers who easily leverage these known vulnerabilities to compromise systems and potentially steal institutional data.

Don't check your personal email while on office systems.

By checking your personal email on the office computer, you are extending the risk profile of the workplace to include your own personal activities. Attacks that target you as an individual, are now naturally extended to the entire University. Our official SUNY OW email account is carefully managed and secured by policies and the vigilance of our ITS team to minimize the risk from suspicious emails, links, and attachments. Once you open your own email account on the office computer, you bypass many of these defenses and render them less effective. If you open that suspicious attachment in your personal email on your office computer, you can infect your system (and eventually many other SUNY OW systems) with malicious software like ransomware that may prevent you or your colleagues from performing their daily duties.

If you follow these few common pearls of IT wisdom, you will help us maintain a much more secure and productive OW workplace. Remember, if you are working handling our University's non-public information, you play a very big part in it's protection and safeguard. Let's all of us work to make it as difficult as possible for attackers to affect our daily operations at SUNY Old Westbury.

Provided By:

Information Technology Services **Division of Business & Finance** **Evan Kobolakis, CIO** **Len Davis, Sr. Vice President & CFO**	**MS-ISAC** Multi-State Information Sharing & Analysis Center	SUNY OLD WESTBURY OWN YOUR FUTURE

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.