Information Security Newsletter

December 2019

Tips Regarding Securely Configuring Your Devices

From the Desk of Milind Samant, ISO

The holiday season is upon us, which means shopping for the latest gadget is in full swing. With the massive number of discounts that are available this year, it makes sense for you to buy that latest smart device, right? However, as impressive as the latest iPhone or gaming computer might be, ensuring you're able to properly secure these devices is more important than ever! Any device, personal or College issued, that connects to the internet is potentially vulnerable and could become compromised. Below are several tips to keep in mind that can help you securely configure your current and new devices.

Secure Configuration Tipsnline Shopping Tips

- **Adjust Factory-Default Configurations and Change Default Passwords**
  Passwords are a common form of authentication and are often the only barrier between cybercriminals and your personal information. Some internet-enabled devices are configured with default passwords to simplify setup. But did you know those passwords can easily be found online? To better secure your digital devices it's important to change the factory-set default password. Be sure to replace it with a strong and unique password or passphrase for each account.
- **Secure your Wi-Fi Network with Encryption**
  Your home's wireless router is the primary entrance for cybercriminals to access your connected devices. To enhance your defenses, use Wi-Fi Protected Access 3 (WPA3). WPA3 is currently the strongest form of encryption for Wi-Fi. Other methods are outdated and more vulnerable to exploitation.
- **Double Your Login Protection**
  Enable multi-factor authentication (MFA) to ensure that only the person who has access to your account is you. If MFA is an option, enable it by using a trusted mobile device such as your smartphone, an authenticator app, or a secure token. For instance, with an iPhone you can utilize your screen lock feature with a pin or password.
- **Disable Location Services and Remote Connectivity**
  Location services might allow anyone to see where you are at any given time. Consider disabling this feature when you are not using your device to further secure your private information. Additionally, most mobile devices are equipped with wireless technologies such as Bluetooth that can be used to connect to other devices or computers. Consider disabling these features when not in use as well!
- **Don't Broadcast Your Wi-Fi Network Name**
  To prevent outsiders from easily accessing your network, avoid publicizing your Wi-Fi network name, or service set identifier (SSID). All Wi-Fi routers allow users to disable broadcasting their device's SSID. Doing so will make it more difficult for attackers to find a network. At the very least, change your SSID to something unique. Leaving it as the

manufacturer’s default could allow a potential attacker to identify the type of router and possibly exploit any known vulnerabilities.

- **Install Firewalls on Network Devices**
  Consider installing a firewall on all the computers you connect to the network. Often referred to as host or software-based, these firewalls inspect and filter a computer’s inbound and outbound network traffic based on a predetermined policy or set of rules. Most modern Windows and Linux operating systems come with a built-in, customizable, and feature-rich firewall. Additionally, most vendors bundle their end point protection software with additional security features such as parental controls, email protection, and malicious website blocking.

- **Remove Unnecessary Services and Software & Install Antimalware Software**
  Disable all unnecessary services to reduce the attack surface of your devices. Unused or unwanted services and software can create security holes on a device’s system, which could lead to an increased attack surface. Additionally, a reputable end point protection software application is an important protective measure against known malicious threats. It can automatically detect, quarantine, and remove various types of malware, such as viruses, worms, and ransomware.

- **Update and Patch Regularly**
  Manufacturers will issue updates as they discover vulnerabilities in their products. The perfect example being all of the update notifications you receive on your iPhone! Configuring your device to receive automatic updates makes this easier for many devices, such as computers, phones, tablets, and other smart devices. However, if you need to manually update your device, make sure you are only applying updates directly from the manufacturer (i.e. Apple), as third-party sites and applications are unreliable and can result in an infected device.

I would like to take this opportunity to wish you all a successful conclusion of the Fall semester and an enjoyable, restful break. Happy Holidays!

Reminders….

- ***Set a strong password:*** *Use at least 8 characters in upper and lower case, numbers, and symbols.*
- ***K**eep 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:

Information Technology Services **Division of Business & Finance** **Evan Kobolakis, CIO** **Len Davis, Sr. Vice President & CFO**	NATIONAL CYBERSECURITY ALLIANCE	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.