Information Security Newsletter

September 2018

Avoiding Different Types of Malware !!

From the Desk of Milind Samant, ISO

When we use our personal or OW-provided digital devices to browse the Internet and work on emails, we also expose them to potential malware (malicious software). Malware is any software that is designed to cause damage, or provide unauthorized access to devices or networks. Malware comes in many forms, all of which can have negative effects. With a little extra vigilance, some good habits and practices, the likelihood that your device will become infected with malware can be minimized. Below, we will explore a few common types of malware, their impacts, and as some tips and practices that can help you as you go about your connected life.

Common Types of Malware and Their Effects

Ransomware – Ransomware is malware that stops you from being able to access your files, usually by encrypting them, and then requests payment to decrypt the files, restoring your access. Most commonly, ransomware asks for payment in bitcoin, which is a popular cryptocurrency. Unfortunately, paying the ransom does not guarantee restoring your access.

Trojan Horses (a.k.a. trojans) – This malware takes its name from the classic story of the Greek army sneaking soldiers into the city of Troy hidden inside a large wooden horse. Trojans of the malware variety behave in much the same way, by appearing to be legitimate apps or software that you want to install. Some trojans allow an attacker full access to your device, others steal banking and personally sensitive information, and others are simply used to download additional malware, like ransomware.

Keyloggers – This type of malware records your keystrokes and sends them to a cyber threat actor, giving them access to your usernames, passwords, and any other sensitive information you have entered using your keyboard. With this information, the cyber threat actor can access your online accounts or commit identity theft.

Tips and Practices for Avoiding and Surviving a Malware Infection

- ***Update and patch your devices and software***. Vendors release updates and patches in order to fix security issues, not just to fix functionality! Many types of malware can be foiled by keeping your software up-to-date by accepting the updates when you get a notice about them.

- ***Never click suspicious or untrusted links.*** Even if the URL comes from a company or person you know, it is always safest to manually type in their URL. At the least, hover over the link to discover where it's really sending you, as some malicious actors send emails that look convincing. This advice is also true for links in emails, documents, and on social media platforms, as malicious links are commonly posted to such sites.

- ***Only download from trusted sources.*** When looking to download an app or software, only do so from a trusted vendor or source. On mobile devices, ensure that you only download apps from the Google Play store and Apple App Store, which are the trusted sources for Android and iOS devices.

- ***Backup your data and be sure the backups are good!*** Backing up your data, whether by doing a complete backup of your whole device or just key files, is the best way to protect those important files and pictures against ransomware and other data loss.

- ***Use antivirus and other protective software on your device.*** If your computer or tablet has built in protections like antivirus or a firewall, ensure you have those enabled. Otherwise, buy or download an antivirus product from a trusted vendor. This is important for your computers, tablets and your smartphones!

- ***Configure your devices with some security in mind.*** By setting up your devices with some basic security settings enabled, you will not only protect against some malware, but against other forms of malicious activity and access.

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, 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

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.