Information Security Newsletter

May 2017

Are You Really Secure Online?

From the Desk of Milind Samant, ISO

Browsing the web and interacting with websites in a secure fashion is immensely important in today's digitally connected world. Everyday things like checking emails, entering student's grades, dealing with Financial Aid information, health records, online banking, and submitting your taxes involve sharing financial and sensitive information online. This makes browsing securely something that everyone at SUNY Old Westbury should consider more closely. Below ITS will explore some ways to connect to the Internet and browse websites securely, as well as how you can double check that you are being secure while transmitting or receiving non public information.

Use a Secured Wi-Fi Network

Wi-Fi access is widely available, but many of the free connections are to unsecured public Wi-Fi network that will leave the information travelling unencrypted! On an unsecured public Wi-Fi network, cyber criminals can easily access the data you are transmitting due to the fact that your information is not encrypted.

> How do you know the Wi-Fi network is one you should trust? Ask someone who should know, like the servicedesk folks located at room 0107 in the New Academic Building. There are no rules about naming your Wi-Fi network, so many Wi-Fi networks run by malicious actors use names that you expect to trust. **Ask - don't trust the name!**

A more secure public Wi-Fi network requires a password or credentials to gain access that are provided by someone acting in an official capacity for the local business and the use of encryption. When looking for an available and more secure wireless network, you will see ones using encryption marked with a small lock symbol next to the name of the network. Some businesses that provide free Wi-Fi to customers provide access to their secure networks by providing the credentials or an access code when checking in, making a purchase, or on request.

If you opt to use a public Wi-Fi connection, make sure you understand the risk – others may be able to see what you do. Keep this in mind and do not conduct sensitive transactions or log in using your credentials to any sites affiliated with SUNY Old Westbury (e.g. connect.oldwestbury.edu, mail.oldwestbury.edu, etc.). Not all apps and sites support encryption and other good security practices, which leaves you much more open to many types of cyber-attacks when on a public Wi-Fi connection which is not secure.

Secure Your Information in Transit

Keep an eye out for that little lock icon on your browser, or the “https” in the URL! Sites that are taking security seriously will encrypt the sensitive information you are exchanging with the site. This is a strong way to ensure that your online activities like shopping or submitting personal information are protected.

The small lock icon or “https” at the beginning of the URL are indicators that encryption is currently in use. The lock icon is commonly found in the address bar on the most popular browsers, including Chrome, Firefox, Safari, Edge, and Internet Explorer.

Verify the Website

When you are looking for information online, make sure you are on the website you intended to visit, or are going to the correct site.

One particular sneaky technique used by cyber criminals is called *typosquatting*. Typosquatting is when someone purposely owns a website that is similar to a trusted website but with a typo in the address. For instance, the website “thisissafe” might be trusted, but the website “thisisafe” could be a malicious website using typosquatting. People are often linked to these incorrect, but very closely named websites through phishing emails sent out by malicious actors. Many websites look the same, and sometimes criminals or other unscrupulous folks use the names and logos of trustworthy companies to mislead you. In some forms of attack, a user being led to a false, but convincing copy of a known website will be prompted to enter their legitimate credentials, which are stolen by the malicious actor who set up this ruse.

A good practice is to not click a link that is provided in your emails, and to instead go type the intended website’s address directly into your browser to ensure you get to the right place.

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