# Information Security Newsletter

## April 2019

Share Your

Information With Care!

### *From the Desk of Milind Samant, ISO*

It is very easy to find any information you need in today’s connected world. Have you ever Googled yourself to see what information about you is online? A search can often provide your address history, phone number, age, birthdate, employment information, public records, and social media accounts. Consider what can be done with Personally Identifiable Information (PII) from the perspective of a cyber-criminal looking to commit identity theft or other crimes. Children, teens, and senior citizens are all groups who especially may not realize how vulnerable they are to being a victim of cyber-crime. Senior citizens may be more trusting of the material that is presented to them online. Children and teens are growing up with technology, and may be using it to communicate with each other with only a recreational level of understanding. They may not realize that once you post online, it rarely goes away.
In order to keep information safe or private, we need to take care in sharing it, and teach cyber hygiene to those who may not understand its importance. Below, please find examples of how people are asked to provide information, or how we share information that should be kept private:

**Store Loyalty And Other Accounts Online** – When you sign up for a store loyalty program or other online accounts, you are asked to provide information such as name, address, phone number, birthdate, email address, etc. By providing this, you can get discounts on the merchandise they are selling, or can receive promotions by email. However, is that information you provide kept private, or is it sold to other companies so they can market to you? Read the terms of use and privacy policy before signing up for such a program.

**Phishing Emails** – Phishing is a cybercrime that targets individuals or institutions through email, text, or social media. The goal is to convince those who have been targeted to provide sensitive data such as personal information, account details, credit card numbers, and passwords. The information can be used to initiate illegitimate money transfers, bogus credit card charges, and send unsolicited emails. It is called “phishing” because, like real-life fishing, the scam involves “casting” (sending out digital messages) and “reeling in” those who are fooled by the phony messages and begin cooperating (unknowingly) with the criminals involved. Unlike email spam, which still accounts for over fifty percent of all email employees receive every day, phishing emails have become much more common targeting higher educational institutes since most faculty and staff find it difficult to identify phishing emails.

**Fraudulent Phone Calls (Vishing)** – Criminals may call saying they are from Microsoft or another device/software company, telling you that your software has expired or your device is infected with malware. They may ask for money to renew a license, as a method to complete the fraudulent activity. Other criminals may pose as the IRS, pressuring you into paying taxes. Never offer payment information or personal information to someone calling you unsolicited.

Always end the call and attempt to contact the organization through a publicly listed phone number that is legitimate, then see if you need to work with them on a problem.

**Social Media Sites** – These sites provide a relaxed atmosphere where you can chat with friends and family. The issue is that anything you post or share is likely a permanent submission that many others can access online. Oversharing on social media may lead to you voluntarily give up answers to account security questions, like the color of your car or the town where you were born. With all this information about you on social media, be sure to set your account privacy settings so only friends can view your content. Lastly, consider deleting old, unused social media accounts to cut down on your digital footprint. Whenever communicating with people or posting online, avoid sharing too much. When receiving emails, mail or calls asking for sensitive information (birthdate, social security number, credit card, etc.), always contact them at the legitimate address or phone number you normally use for that organization. Do not share information if you do not initiate the communication!

Below are resources on protecting privacy and identity along with practices for online security.

**Resources:**

Federal Trade Commission:
https://www.consumer.ftc.gov/topics/privacy-identity-online-security

https://www.consumer.ftc.gov/articles/0033a-share-care

Stay Safe Online:
https://staysafeonline.org/

Family Online Safety Institute:
https://www.fosi.org/good-digital-parenting/ftc-share-care/

**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**<br>**Division of Business & Finance**<br>**Evan Kobolakis, CIO**<br>**Len Davis, Sr. Vice President & CFO** | NATIONAL CYBERSECURITY ALLIANCE | SUNY OLD WESTBURY<br>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.*