Information Security Newsletter

March 2019

How to Spot and Avoid Common Scams!

From the Desk of Milind Samant, ISO

Have you ever received an email from someone claiming to be royalty? In their email, they tell you that they will inherit millions of dollars, but need your money and bank details to get access to that inheritance. You know that the email isn't legitimate, so you delete it, yet there are many more scams being perpetrated by criminals that sound more believable and aren't as easy to spot. Learning to identify and avoid these scams is the first step in protecting yourself from these fraudulent schemes. The world today is full of cybercriminals launching both phishing emails as well as the old tactic of tried-and-true phone scams. Protecting not only your finances, but also your data from these scams is more important now than ever.

Phone Scams

Scammers who operate by phone can seem legitimate and are typically very persuasive! To draw you in to their scam, they might:

- Sound friendly, call you by your first name, and make small talk to get to know you,
- Claim to work for a company or organization you trust such as: a bank, a vendor you use, the police department, or a government agency such as the IRS,
- Threaten you with fines or charges that must be paid immediately,
- Mention exaggerated or fake prizes, products, or services such as credit and loans, extended car warranties, charitable causes, or computer support,
- Ask for login credentials or personal sensitive information,
- Request payments to be made using odd methods, like gift cards,
- Use prerecorded messages, or robocalls.

If you receive a suspicious phone call or robocall, the easiest solution is to hang up. You can then block the caller's phone number and register your phone number on the National Do Not Call Registry (https://www.ftc.gov/donotcall).

Email Scams

Phishing emails are convincing and trick many people into providing personal data. These emails tend to be written versions of the scam phone calls described above. Some signs of phishing emails are:

- Imploring you to act immediately, offering something that sounds too good to be true, or asking for personal or financial information,

- Emails appearing to be from executive leadership (such as deans, chairs, vice presidents, president, etc) where you work equesting information about your whearabouts or colleagues location,
- Unexpected emails appearing to be from people, organizations, or companies you trust that will ask you to click on a link and then disclose personal information. Always hover your mouse over the link to see if it will direct you to a legitimate website,
- Typos, vague and general wording, and nonspecific greetings like “Dear customer”.

Beware that many scam and phishing emails look legitimate! If you’re unsure about an email you received, there are some steps you can take to protect yourself:

- Do not click links or open attachments in emails you were not expecting,
- Do not enter any personal, login, or financial information when prompted by an unsolicited email,
- Do not respond to or forward emails you suspect to be a scam,
- If in doubt, contact the person or organization the email claims to have been sent by using contact information you find for yourself on their official website,

If you get scam phone calls or phishing emails at home, hang up or delete the emails. If you get scam phone calls or phishing emails at SUNY Old Westbury systems, please inform the ServiceDesk so that they can help protect others from these scams! Additionally, please educate your loved ones about these scams, since they are becoming more and more common.

Resources:

1. https://www.consumer.ftc.gov/articles/0076-phone-scams
2. https://staysafeonline.org/stay-safe-online/online-safety-basics/spam-and-phishing/

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.