

Information Security Newsletter

December 2017



Avoiding Holiday Scams

From the Desk of Milind Samant, ISO

The holiday season is a great time to make charitable gifts to support the causes we care about, and charities often run end-of-year fundraising campaigns. However, criminals take advantage of this fact and run scams and frauds of their own to fool patrons into giving them money instead. Below are some common scams and frauds used by cybercriminals and some tips on how to avoid them. If you can spot these seasonal tricks, you are more likely to ensure your donation goes where you intend it to go.

Fake Charity Websites

One of the most convincing ways for cybercriminals to exploit charitable giving is by creating convincing charity websites. These websites are in fact fraudulent and may copy an existing charity's site or use the charity's name and branding. While few techniques are fool proof for detecting fake or malicious websites, try to follow these recommendations:

- Whenever possible, browse directly to the charity by entering the charity's URL directly into your browser's address bar.
- If you are not sure of the charity's URL, an Internet search can help, but instead of automatically clicking on the first link, look at the top few links. If the top link is what you want, great, but if you see several very similar links this could indicate one of them is a potentially fraudulent website.
- Carefully study the website's URL for typos, such as two "v" characters in place of a "w" or an "i" instead of an "l." If you're not sure about a potential typo, try changing to all capitals or a different font.
- Fraudulent charity websites frequently use domain names and email addresses that sound legitimate. You can do a little research into what the correct domain name and email address should be by looking into the organization using resources recommended by the Federal Trade Commission in their [charity guide](#), or through resources like GuideStar, Charity Navigator, and Charity Watch.

Pleas for Donations via Social Media

Scammers commonly impersonate staff from major charities via social media channels, as this makes it easier for them to impersonate someone else. Avoid making donations through social media and never send your personal or payment information in a social media message. Instead, consider heading directly to a charity's established website.

In addition to traditional charity scams at this time of year, social media is also susceptible to the spread of a variety of pyramid schemes and other charity scams. Pyramid schemes involve the simple but unsustainable premise of receiving more than you give.

One of the most common schemes on social media right now involves 7 bottles of wine.

You receive the message indicating that to participate you should send one bottle of wine to the person who tagged you and post the message, tagging 6 other people who will each send you a bottle.

Another scheme purports to be from a sick child who wants something – holiday cards for example and asks you to send a card and share the post with all your friends so that they will send a card, too. If you come across one of these viral posts, let it stop with you! Don't share it, repost it, or send anything along, and do take a moment to educate your friends and colleagues at SUNY Old Westbury!

When donating to a charity, make sure that the charity is a registered charity under U.S. or international tax law. U.S. 501 charities have to make certain information public and you can look the charity and its information up under any of the several charity tracking websites.

Wishing you an enjoyable and safe winter break and hope everyone finds time to relax, have fun, and renew themselves for the new semester and new year 2018.



Reminders....

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

<p>Information Technology Services Division of Business & Finance Evan Kobolakis, CIO Len Davis, Sr. Vice President & CFO</p>	 <p>MS-ISAC Multi-State Information Sharing & Analysis Center</p>	 <p>SUNY OLD WESTBURY OWN YOUR FUTURE</p>
---	---	---

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.