

Information Security Newsletter

March 2018



Staying Safe from Tax Scams

From the Desk of Milind Samant, ISO

Though Benjamin Franklin is often quoted as saying “in this world, nothing can be said to be certain, except death and taxes,” an updated version for the current day would need to include tax scams. As people nationwide seek to file their tax returns, cybercriminals attempt to take advantage of this with a variety of scams. Hundreds of thousands of U.S. citizens are targeted by tax scams each year, often only learning of the crime after having their legitimate returns rejected by the Internal Revenue Service (IRS) because scammers have already fraudulently filed taxes in their name. The IRS reported a 400% rise in phishing scams from the 2015 to the 2016 tax season. In the state, local, tribal, and territorial government sector during 2017, approximately 30% of all reported data breach incidents were related to the theft of W-2 information, which was likely used for tax fraud.

How is Tax Fraud Perpetrated?

Unfortunately, much of someone’s personal information can be gathered from multiple locations online with almost *no verification* that the right person is receiving the information. Criminals know this, so they use this trick to get individual’s personal information from a variety of websites and use the information to file a fake tax refund request! If a criminal files a tax return in your name before you do, they will file it with false information to get a large refund, forcing you to go through the arduous process of proving that you did not file the return and subsequently correcting the return. Once they have your personal information, criminals can continue to commit identity theft well beyond the tax season.

Another favorite technique used by criminals during the tax season is sending phishing messages indicating that a new copy of your tax form(s) is available. These emails often impersonate state, local, tribal, and territorial government comptroller and/or IT departments. They might include a link to a phishing website that uses our SUNY Old Westbury’s logo and the email might even have the right signature line. If you fill out or attempt to login into the phishing website, the criminals will be able to see your login name and password, which they can then use to try and compromise your other accounts. The more information they gather from you, the easier it is for them to use the information to file a fake tax return in your name.

Tax fraudsters also impersonate the IRS and other tax officials to threaten taxpayers with penalties if they do not make an immediate payment. This contact may occur through websites, emails, or threatening calls and text messages that look official but are not. Sometimes, criminals request their victims pay the “penalties” via strange methods like gift cards or prepaid credit cards. It is important to remember:

- The IRS will not initiate contact about payment with taxpayers by phone, email, text messages, or social media without sending an official letter in the mail first.

What Can You Do?

Here are some basic tips to help you minimize the chances of becoming a victim of a tax scam:

- If you haven't already, file your taxes as soon as you can...before the scammers do it!
- Be aware of phone calls, emails, and websites that try to get your information, or pressure you to make a payment. If something seems suspicious, contact the organization through a known method, like their publicly posted customer service line.
- Ignore emails and texts asking for personal or tax information. Be cautious as to whom you provide your information, including your Social Security Number and date of birth.
- Don't click on unknown links or links from unsolicited messages. Type the verified, real organizational website into your web browser.
- Don't open attachments from unsolicited messages, as they may contain malware.
- Check your credit report regularly for unauthorized activity. Consider putting a security freeze on your credit file with the major credit bureaus if you suspect you have been targeted for identity theft.

If you receive a tax-related phishing or suspicious email at work, report it to SUNY OW Service Desk at phishing@oldwestbury.edu or call ext. 3098. The IRS encourages taxpayers to send suspicious emails related to tax fraud to its phishing@irs.gov email account or to call the IRS at 800-908-4490.

If you suspect you have become a victim of tax fraud or identity theft, the Federal Trade Commission (FTC) [Identity Theft website](#) will provide a step-by-step recovery plan. It also allows you to report if someone has filed a tax return fraudulently in your name, if your information was exposed in a major data breach, and many other types of fraud.

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:

Information Technology Services
Division of Business & Finance
Evan Kobolakis, CIO
Len Davis, Sr. Vice President & CFO



MS-ISAC
Multi-State Information
Sharing & Analysis Center



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.