

From the Desk of Milind Samant, ISO

As people seek to file their tax returns this year, cybercriminals will be busy trying to take advantage of this with a variety of scams. According to the Internal Revenue Service (IRS), there was a 60% increase in 2018 in phishing scams that tried to steal money or tax data. The IRS identified 9,557 fraudulent tax returns as of only February 24th, 2018 for the last filing season. As everyone aims to file their returns among all this fraud, the following advice will explain how tax fraud happens and provide recommendations on how to prevent it from happening to you or how to get help if you are unfortunately affected by a tax scam!

How is tax fraud perpetrated?

The most common way for cybercriminals to steal money, financial account information, passwords, or Social Security Numbers is to simply ask for them. Criminals will send phishing messages often impersonating government officials and/or IT departments. They may tell you a new copy of your tax form is available. They may include a link in a very official looking email that goes to a website that uses an official logo and appears legitimate, yet is fraudulent. If you attempt to login into the false website, or provide any personal information, the criminals will see what you type and try to use it to compromise your other accounts and file a false return in your name.

Additionally, much of your personal information can be gathered online from social media or past data breaches. Criminals know this, so they gather pieces of your personal information from a variety of sources and use the information to file a fake tax refund request! If a criminal files a tax return in your name before you do, you will go through the arduous process of proving that you did not file the return and subsequently correcting the return.

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

- Initiate contact by phone, email, text messages, or social media without sending an official letter in the mail first.
- Call to demand immediate payment over the phone using a specific payment method such as a debit/credit card, a prepaid card, a gift card, or a wire transfer.
- Threaten you with jail or lawsuits for non-payment.
- Demand payment without giving you the opportunity to question or appeal the amount they say you owe.
- Request any sensitive information online, including PIN numbers, passwords or similar information for financial accounts.

How can you protect yourself from tax fraud?

- File your taxes as soon as you can...before the scammers do it for you!
- Always be wary of calls, texts, emails, and websites asking for personal or tax data, or payment. Always contact organizations through their publicly-posted customer service line. If they contact you end the call and call the organization on the phone number on their website.
- Don't click on unknown links or links from unsolicited messages. Type the verified, real website address into your web browser. Don't open attachments from unsolicited messages, as they may contain malware.
- Use strong, unique passwords for all your accounts and protect them. Reusing passwords between accounts is a big risk that allows a breach of one account to affect many of them! Keep SUNY OW password different from your personal password.
- Check your financial account statements and your credit report regularly for unauthorized activity. Consider putting a security freeze on your credit file with the major credit bureaus. This will prevent identity thieves from applying for credit or creating an IRS account in your name.

If you receive a tax-related phishing or suspicious email at SUNY OW email address, report it to the ServiceDesk. If you receive a similar email on your personal email account, the IRS encourages you to forward the original suspicious email as *an attachment* 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](#) provides a step-by-step recovery plan. It also allows you to report if someone has filed a 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, 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



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.