March 2014
Volume 9, Issue 3

Protect Yourself from Online Tax Scams

ENTERPRISE INFORMATION SECURITY PROGRAM
Keeping our organization's data safe.

City of Tacoma
Enterprise Information Security Program

Tacoma

From the Desk of Paul Federighi, Chief Information Security Officer

Tax season is in full swing and criminals are seizing the opportunity for scams. Because of the recent major data breaches we've seen in the past few months, which exposed sensitive information on a large scale, we should be even more vigilant about taking steps to minimize our risk of ID theft and other online-related crime. Don't become the next victim.

Scammers leverage every means at their disposal to separate you from your money, your identity, or anything else of value they can get. They may offer seemingly legitimate "tax services" designed to steal your identity and your tax refund, sometimes with the lure of bigger write-offs or refunds. Scams may include mocked up websites and tax forms that look like they belong to the IRS to trick you into providing your personal information.

Vigilance about the security of our online activities is required every day, but is especially important during this time of year. Below are some warning signs to look for and basic precautions you can take to minimize risk.

How To Recognize an Online Tax Scam

- requests personal and/or financial information, such as name, SSN, bank or credit card account numbers or security-related information, such as mother's maiden name, either in the email itself or on another site to which a link in the email directs you;
- includes exciting offers to get you to respond, such as mentioning a tax refund or offering to pay you to participate in an IRS survey;
- threatens a consequence for not responding to the email, such as additional taxes or blocking access to your funds;
- has incorrect spelling for the Internal Revenue Service or other federal agencies;
- uses incorrect grammar or odd phrasing;
- discusses "changes to tax laws" that include a downloadable document (usually in PDF format) that purports to explain the new tax laws (these downloads are populated with malware that, once downloaded, may infect your computer).

How To Avoid Becoming a Victim

- Submit your tax returns as soon as possible in order to prevent someone else from filing under your name.
- Secure your computer. Make sure your computer has the latest security updates installed. Check that your anti-virus and anti-spyware software are running properly and are receiving automatic updates from the vendor. If you haven't already done so, install and enable a firewall.

- Carefully select the sites you visit. Safely searching for tax forms, advice on deductibles, tax preparers, and other similar topics requires caution. Do not visit a site by clicking on a link sent in an email, found on someone's blog, or in an advertisement. The website you land on may look just like the real site, but it may be a well-crafted fake.

- Be wise about Wi-Fi. Wi-Fi hotspots are intended to provide convenient access to the Internet and are not necessarily secure against eavesdropping by hackers. Do not use public Wi-Fi to file your taxes.

- Don't fall prey to email, web, or social networking scams. Common scams tout tax rebates, offer great deals on tax preparation or offer a free tax calculator tool. If you did not solicit the information, it's likely a scam. ***If the email claims to be from the IRS, it's a scam -- the IRS will not contact you via email, text messaging or your social network, nor does it advertise on websites.*** If the email appears to be from your employer, bank, broker, etc., claiming there is an issue with what they reported for you and you need to verify some information, it might be a scam. Do not respond to the email. Contact the entity directly before responding.

- Never send sensitive information in an email. It may be intercepted by criminals.

- Use strong passwords. Cyber criminals have developed programs that automate the ability to guess your passwords. To protect yourself, passwords must be difficult for others to guess, but at the same time, easy for you to remember. Passwords should have a minimum of nine characters and include upper case (capital letters), lower case letters, numbers, and symbols. Make sure your work passwords are different from your personal passwords.

For More Information

The Center for Internet Security's Protect Yourself from Tax Season Identity Theft Scams:
http://msisac.cisecurity.org/resources/guides/tax/

Taxpayer Guide to Identity Theft:
http://www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft

IRS Dirty Dozen Tax Scams for 2014:
http://www.irs.gov/uac/Newsroom/IRS-Releases-the-%E2%80%9CDirty-Dozen%E2%80%9D-Tax-Scams-for-2014;-Identity-Theft,-Phone-Scams-Lead-List

Report Phishing:
http://www.irs.gov/uac/Report-Phishing

Provided By:

CENTER FOR INTERNET SECURITY

STOP | THINK | CONNECT