ENJOY SAFER TECHNOLOGY®

TAX SEASON IS FINANCIAL CRIME SEASON

Tax season is financial crime season

Nine things you need to know about protecting your financial identity

By ESET staff

You see the countdown to April 15 (April 18 this year) as a deadline, but to online criminals it's a window of opportunity. Sensitive financial data is everywhere: taxes filed online, taxpayers accessing banking and investment information, and personal financial records sitting on hard drives. The opportunity is irresistible to online thieves, so business owners who let their guard down during the rush to get their taxes done are susceptible to scam artists.

Tax refund fraud is one of the fastest-growing crimes in the U.S., and is expected to hit a whopping $21 billion in 2016. That's up from just $6.5 billion two years ago. To pull off the scam, all a crook needs is some personal information and your Social Security number to file a false tax return and claim a refund on your behalf.

IRS impersonation scams have snared more than 3,000 victims over the last few years, padding fraudsters' pockets to the tune of $14 million. How does it work? The criminal calls you, presents enough personal information to convince you that he or she is an IRS employee, and pressures you to pay the taxes that you supposedly owe via a prepaid debit card or wire transfer.

Identity thieves often send fake emails purporting to be from the IRS in order to trick victims into disclosing personal information.

Your financial identity is yours and yours alone. You need to protect it to safeguard yourself, your business, and your livelihood. The following are some steps you can take to keep the scammers at bay during financial crime season—and all year round.

1. Sweep your computer before you access or transmit financial data.

Before you work on your taxes, work with financial data on your computer, or visit banking or other financial sites, update your antivirus/antimalware software and run a scan. The little bit of extra time it takes is well worth it when you consider the consequences of a keylogger or other malware grabbing your passwords, account numbers, Social Security number, or other personal data that could be used to steal your financial identity.

2. Use only a secure browser when banking or shopping online.

Every bit of personal information is potentially useful to a crook. A banking site, shopping site, or any other site that trades in personal financial data or sensitive information should support secure, encrypted browsing. Any site that doesn't simply isn't worth the risk. You can tell the session is secure when the URL begins with https, not just http. For extra safety, look for security software that includes Banking and Payment Protection, which automatically opens a new, secure browser for you when you're making financial transactions online.

3. Don't give out any personal financial information unless you have logged into the banking or tax site directly.

If you get an email from a bank, shopping site, or any other source that asks you to verify passwords or enter personal information, don't click on the link. Type the site's URL into the address bar yourself and log in, or use the phone to contact them. Deceptive emails and phony web sites are easy for crooks to fake. Security software that protects against these phishing schemes adds an extra layer of security should you ever let your guard down.

4. Log out of online tax-filing or banking sessions as soon as you're finished.

Leaving a session open while you do other work on your computer, take a phone call, or step away from your computer is an open invitation for crooks, and they don't have to have control of your computer to hijack your session. Always close your browser completely after you've visited any site that requires a log-in or deals with your personal information.

5. Don't file returns or access financial sites from a coffee bar, airport, hotel, or other Wi-Fi hot spot.

A public Wi-Fi hot spot is wide open for thieves who can steal information or plant malware on your computer. Never use them when you're sending or working with your financial or other personal information. Be especially careful with your tax return—complete with your Social Security number, it's a gold mine for identity thieves. If you use public hotspots at all, for any purpose, install security software that includes a firewall.

6. Consider encrypting the information you store or send.

Encryption software is simple to use, and protects your sensitive personal information from prying eyes. Recipients of your emails can open them normally. If you store tax or financial records on your computer, store them in a folder with an innocuous or misleading name, and use a file encryption program to provide additional security in case your machine becomes compromised.

7. Delete, instantly, emails that appear to come from the IRS.

The IRS does not initiate email conversations or use the Web to ask for personal information. All of its communication comes via traditional postal mail. If you get an unexpected email purporting to be from the IRS, it most certainly is a scam. Even if you do no more than open the email and close it, that's all it takes for malware to be planted on your computer and start stealing your financial information. And never, ever respond to an email that asks for your Social Security number, a PIN, password, or bank account number—or directs you to a site prompting you to enter that kind of information.

8. Protect mobile devices, too.

Your mobile device might contain financial information, emails with account updates from your bank, or links that allow a thief to access your bank account. If you haven't done so already, lock your phone with a password, and invest in security software that protects it from malware and safeguards your information in case of loss or theft.

9. Update your security programs, web browsers, and third-party programs regularly.

It's standard advice, but it bears repeating: update regularly, so you get the latest security patches. Spyware and malware take advantage of vulnerabilities in software to gain a foothold, install, and spread silently. New vulnerabilities are discovered all the time, and your mission is to keep up with the patches before the criminals can exploit them. Make sure your operating system and all web browsers you use are up to date, and pay special attention to browser plug-ins.

By following these tips, and combining a little extra vigilance with the right security software, you can protect your computing devices, your financial identity, and your livelihood. And there's no better time to act than right now—before the April 18 deadline is staring you in the face.

About ESET Multi-Device Security

Implementing ESET Multi-Device Security (EMDS) is an easy, effective way to protect all your Windows, Mac, and Android devices in your home workspace or small office. With a single license, you can protect up to 10 computers and Androids. EMDS secures Bring Your Own Device workers, adds antitheft protection to mobile devices, and protects privacy on public Wi-Fi. With cross-platform versatility in a package that's easy to install and implement, you can rest easier, and focus on running your business—not your security system.

For over 25 years, ESET® has been developing industry-leading security software for businesses and consumers worldwide. With security solutions ranging from endpoint and mobile defense to encryption and two-factor authentication, ESET's high-performing, easy-to-use products give users and businesses the peace of mind to enjoy the full potential of their technology. ESET unobtrusively protects and monitors 24/7, updating defenses in real time to keep users safe and businesses running uninterrupted. For more information, visit www.eset.com.

ENJOY SAFER TECHNOLOGY®