UTHSC G.U.A.R.D.

February 2018

IN THIS ISSUE

Stay Safe from Cybercrime During Tax Time

by Chris Madeksho, Information Security Coordinator

Tax season, everyone's favorite time of year, is already upon us. According to the Federal Trade Commission (FTC), tax-related identity theft – when a criminal uses someone else's Social Security number along with other personal data to file an income tax return (refunds). This is the most common type of identity theft. The Internal Revenue Service (IRS) indicates that phishing schemes continue to lead its "dirty dozen" list of 2017 tax scams.

The first step is realizing which scams are out there that target taxpayers. If you protect yourself against these unscrupulous schemes, your identity and tax return will be more safe and secure

IRS-IMPERSONATION PHONE SCAMS - Callers impersonating IRS officials will insist you owe money and for you to pay immediately, in the form of a gift card or wire service. The real IRS will not call you nor demand immediate payment; in general, they will mail you a bill for any amount owed.

INCREASE IN PHISHING SCHEMES - Cybercriminals will attempt to steal your personal information. Watch out for unsolicited emails, text messages, social media posts or fake websites that may prompt you to click on a link asking to share valuable personal and financial information.

FRAUDULENT TAX RETURNS - The FTC strongly recommends filing your tax return as soon as possible. The IRS only accepts one tax return per Social Security number. If the file is yours, it becomes impossible for a fraudster to submit another return with your personal information.

TAX PREPARER FRAUD - Some unsavory individuals may target unsuspecting taxpayers and the result can be refund fraud and/or identity theft. The IRS reminds anyone filing a tax return that their preparer must sign with their IRS preparer identification number.

If you would like more information, please contact the Information Security Team at itsecurity@uthsc.edu or (901) 448-1880.

IRS Tax Schemes

Check out these scams that are headed your way

Cybersecurity and the Home

Learn some tips on how to make your home more secure

Creating a Cybersecure Home

by Matt Bromiley, Consulting Director, SANS Security Awareness

Several years ago, creating a cybersecure home was simple; most homes consisted of nothing more than a wireless network and several computers. Today, technology has become far more complex and is integrated into every part of our lives, from mobile devices and gaming consoles to your home thermostat and your refrigerator. Here are four simple steps for creating a cybersecure home.

Your Wireless Network

Almost every home network starts with a wireless (or Wi-Fi) network. This is what enables all your devices to connect to the Internet. Most home wireless networks are controlled by your Internet router or a separate, dedicated wireless access point. They both work the same way: by broadcasting wireless signals. The devices in your house can then connect via these signals. This means securing your wireless network is a key part of protecting your home. We recommend the following steps to secure it:

- Change the default administrator password to your Internet router or wireless access point.
- Ensure that only people you trust can connect to your wireless network.
- Ensure the password used to connect to your wireless network is strong and that it is different from the admin password.

Your Devices

The next step is knowing what devices are connected to your wireless home network and making sure all of those devices are secure. This used to be simple when you had just a computer or two. However, almost anything can connect to your home network today, including your smartphones, TVs, gaming consoles, baby monitors, speakers, or perhaps even your car. Once you have identified all the devices on your home network, ensure that each one of them is secure. The best way to do this is ensure you have automatic updating enabled on them wherever possible.

Passwords

The next step is to use a strong, unique password for each of your devices and online accounts. The key words here are strong and unique. Tired of complex passwords that are hard to remember and difficult to type? So are we. Use a passphrase instead. This is a type of password that uses a series of words that is easy to remember, such as "Where is my coffee?" or "sunshine-doughnuts-happy-lost". The longer your passphrase is, the stronger. A unique password means using a different password for each device and online account. This way, if one password is compromised, all your other accounts and devices are still safe. Finally, enable two-step verification whenever available, especially for your online accounts. Two-step verification is much stronger. It uses your password, but also adds a second step, such as a code sent to your smartphone or an app on your smartphone that generates the code for you. Two-step verification is probably the most important step you can take to protect yourself online, and it's much easier than you think.

Backups

Sometimes, no matter how careful you are, you may be hacked. If that is the case, often the only way you can recover your personal information is to restore from backup. Make sure you are doing regular backups of any important information and verify that you can restore from them. Most mobile devices support automatic backups to the Cloud. For most computers, you may have to purchase some type of backup software or service, which are relatively low- priced and simple to use.