

HOME CYBER DEFENSE

ARE YOU SAFE FROM CYBER CRIME?

WEEKLY

Volume #4 - Issue #147

February 16th, 2018

This is a weekly publication dedicated to your personal cyber security. Our newsletter is designed to help the public recognize and avoid cyber threats while they are online. If you are not a subscriber, please go to HomeCyberDefense.net to sign up.

Protecting Your Tax Return



The IRS has recently begun to accept 2017 tax returns. With all of the data breaches that occurred in the past year, this may be the year that you will want to file early and to take some extra precautions.

If a criminal obtained your name, date of birth, and Social Security number, they may be able to file a tax return or do other unscrupulous acts using your good name. But, even though your information was compromised, it does not necessarily mean that this will happen. However, do not let your guard down. Pay attention and do all that you can to protect yourself from falling victim to identity theft.

If you file early, you have a better chance that your legitimate return will be processed before a fraudulent return is done. To combat this, the IRS is trying something new this year with our W-2s. Some will have a special verification code to prove it is legitimate. But not all employers will be using this yet. Thus, when you file your return, it is especially important to make sure that you are keeping your information as secure as possible. Many of us receive W-2s and other tax documents via email or online, or we might file our taxes online. Whether accessing documents or filing online, it is critical that you are using well protected, updated computers and software, secure networks, and that you are using extra strong passwords. Be careful of phishing emails or phone calls that may seem legitimate, but are not. When in doubt, do not open or click on links, nor respond to requests for personal information until you can check things out with a reputable source.

Other ways to protect your tax return:

Don't fall for scams.

If someone calls or emails claiming to be from the Internal Revenue Service (IRS) asking for personal information, don't give it. The IRS will only request information by mail, so if you receive

a call, email or text message claiming to be from the IRS and asking you to provide personal details, don't – it is most likely a scam.

Research your tax preparer.

Be very careful about choosing a tax preparer. Only hire individuals who have the proper IRS credentials, then request their full name and tax certification documentation. Be sure to keep copies of it with your tax paperwork even after filing. Even if you're using an e-filing service, researching the provider is just as important.

Protect your Social Security number.

Leave your Social Security card at home and only give out the number when absolutely required. If you are requested to provide it on a form, ask the company why they need it and if it is necessary, because this is often optional.

Consider signing up for protection services.

Signing up with a service that specializes in identity theft protection could help you to stay on top of keeping your personal information safe by receiving alerts immediately if any fraudulent activity occurs.

Shred your personal records.

Destroy old tax forms, monthly financial statements and other documents that include your personal information once deemed unnecessary. Switching to online delivery is another safe bet so your documents are less likely to end up in places where they can be stolen, like your mailbox or recycling bin.

If you do choose online delivery, make sure that any personal accounts storing this information are appropriately secured. Lock Down Your Login: Your usernames and passwords are not enough to protect key accounts like email, banking and social media. Strengthen online accounts and use strong authentication tools – like biometrics, security keys or a unique, one-time code through an app on your mobile device – whenever offered.

Attacks on consumer's tax returns are increasing at a rapid rate. Make sure you take precautions to protect yourself.

This Week's Cyber Alerts:

Alert Issued 2/15/18 [Skype Can't Fix a Nasty Security Bug without a Massive Code Rewrite](#)

Alert Issued 2/14/18 [Microsoft to add Windows Defender Advanced Threat Protection support for Windows 7](#)

Alert Issued 2/13/18 [Killing Passwords in Windows 10 S is one of 7 big changes in Windows 10](#)

Alert Issued 2/12/18 [This Phishing Trick steals your Email and then Fools your Friends into Downloading Malware](#)

Alert Issued 2/10/18 [Equifax Breach may have Exposed More Data than First Thought](#)

Alert Issued 2/9/18 [73 Percent of Firms Fail Cybersecurity Readiness Tests](#)

Alert Issued 2/9/18 [2017 Smashed World's Records for Most Data Breaches, Exposed Information](#)

Alert Issued 2/8/18 [Hacker Easily Bypasses Windows 10 Anti-ransomware Protection with this Trick](#)

Alert Issued 2/8/18 [42 Percent of the Most Popular Websites are Vulnerable to Cyberattacks](#)

Thank you for subscribing to our email and I hope the information we have shared will make your online life a little easier.



Copyright © 2015-2017 House of File Technologies