March 2015
Volume 10, Issue 3

Avoiding Online Tax Scams

NH Department of Information Technology
www.nh.gov/doit/cybersecurity

It's tax season, which means it's also time for tax scams, with numerous online scams that attempt to steal people's tax refunds, bank accounts, or identities. Last year, the Internal Revenue Service (IRS) estimates it paid $5.2 billion in fraudulent identity theft refunds in filing season 2013.[1] Websense Security Labs reported in 2014 it saw approximately 100,000 IRS-related scams in circulation every two weeks.[2]

This year, we need to be especially careful in light of the Anthem Breach, in which data from approximately 80 million customers was exposed, triggering new phishing attacks offering false claims of credit monitoring services.

Users who have already filed their taxes this season can still be vulnerable to tax-related scams. Many schemes take advantage of users by alleging to have information about the filer's refund, or noting a problem with the return that was previously filed.

One scam that has already been impacting users this season involves phishing emails claiming to be from Intuit's TurboTax. The emails prompt users to click on links to verify their identity or update their accounts in an attempt to download malware to the victim's machine, or steal data such as Social Security numbers or financial information.

Below are some of the most common email scams users should be cautious about:

- **The email says the user is owed a refund** and should forward a bank account number where the refund may be deposited. Once the scammer has the bank account information, that account will see a big withdrawal, not a deposit.

- **The email contains exciting offers** or refunds for participating in an "IRS Survey." This fake survey is actually used to acquire information to perform identity theft.

- **The email threatens the user** with fines or jail time for not making an immediate payment, or responding to the email.

- **The email includes a "helpful" downloadable document** (e.g. "new changes in the tax law," a tax calculator, etc.). In reality, the download is a malicious file intended to infect your computer.

How To Avoid Becoming A Tax-Scam Victim

- **Do not respond to emails appearing to be from the IRS.** The IRS **does not initiate** taxpayer communications through email or social media to request

[1] http://www.gao.gov/products/GAO-14-633

[2] http://money.cnn.com/2014/03/18/smallbusiness/tax-cyberscams/

personal or financial information. If you receive an unsolicited email claiming to be from the IRS, send it to phishing@irs.gov.

- **Do not respond to unsolicited emails and do not provide sensitive information via email.** If the email appears to be from your employer, bank, broker, etc., contact the entity directly. Do not open any attachments or click on links contained in unsolicited or suspicious emails.

- **Carefully select the tax sites you visit.** Use caution when searching online for tax forms, advice on deductibles, tax preparers, and other similar topics. 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.

- **Secure your computer.** Make sure your computer has all operating system and application software updates. Anti-virus and anti-spyware software should be installed, running, and receiving automatic updates. Ensure you use a strong password and different passwords for each account.

Resources

IRS 2015 Dirty Dozen Tax Scams: www.irs.gov/uac/Newsroom/IRS-Completes-the-Dirty-Dozen-Tax-Scams-for-2015

What to Do if Your Identity is Stolen- FTC Guidebook: http://www.consumer.ftc.gov/articles/pdf-0009-taking-charge_0.pdf

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

Tax Scams/Consumer Alerts: www.irs.gov/uac/Tax-Scams-Consumer-Alerts

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

Provided By:

Center for Internet Security
MULTI-STATE Information Sharing & Analysis Center

STOP | THINK | CONNECT

The information provided in the Monthly Security Tips Newsletter is intended to increase the security awareness of an organization's end users and to help them behave in a more secure manner within their work environment. While some of the tips may relate to maintaining a home computer, the increased awareness is intended to help improve the organization's overall cyber security posture. This is especially critical if employees access their work network from their home computer. Organizations have permission and are encouraged to brand and redistribute this newsletter in whole for educational, non-commercial purposes.
Disclaimer: These links are provided because they have information that may be useful. The Center for Internet Security (CIS) 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. The opinions and statements contained in such resources are those of the author(s) and do not necessarily represent the opinions of CIS.