February 2016
Volume 11, Issue 2

Avoiding Online Tax Scams

From the Desk of Thomas F. Duffy, Chair, MS-ISAC

It's tax season, which means it's also time for tax scams. Some tax scams occur when fraudulent tax returns are filed in the victim's name while other variants occur when the malicious actors call the victim and pretend to be Internal Revenue Service (IRS) agents. In addition, there are malicious actors who use the tax season to spread malware and phishing emails.

Tax scams where the malicious actor files the return in the victim's name include both identity theft and identity fraud, as well as tax fraud. This scenario occurs when the malicious actor finds or receives information about the tax filer, including the filer's name, address, date of birth, and Social Security Number. The malicious actor then uses this information to file a malicious tax return, citing as many deductions as possible, in order to create as large a tax return as possible.

The other variant of tax scams occur when the malicious actor contacts the victim and tries to convince the victim to do something, such as immediately paying a fine or providing their financial information so a refund can be issued. In these instances the malicious actor uses what they know about the victim, often information gained for a data breach or social networking website, to convince the victim that the caller has access to the victim's tax information. Frequently during these calls the caller will pretend to be an IRS agent.

In the third type of tax scam, malicious actors use tax related spam, phishing emails, and fraudulent websites to trick victims into providing login names, passwords, or additional information, which can be used in further fraud. Other emails or websites may download malware onto the victim's computer.

What to Watch Out For

- Watch for "spoofed" websites that look like the official website but are not.
- Don't be fooled by unsolicited calls. The IRS will never call to demand an immediate payment or require you

If you owe taxes, the IRS will first mail you a bill, before contacting you through another medium.

to use a specific payment method such as pre-loaded debit or credit cards, or wire transfers. They will never claim anything is "urgent" or due immediately, nor will they request payment over the phone.

- The IRS will not be hostile, insulting, or threatening, nor will they threaten to involve law enforcement in order to have you arrested or deported.
- Sometimes malicious actors change their Caller ID to say they are the IRS. If you're not sure, ask for the agent's name, hang up, and call the IRS (or your state tax agency) back using a phone number from their official website.

Recommendations

If you believe you are the victim of identity theft or identity fraud, there are a couple of steps you should take:

1. File a report with your local law enforcement agency.
2. File a report with the Federal Trade Commission (FTC) at www.identitytheft.gov.
3. File a report with the three major credit bureaus and request a "fraud alert" for your account (Equifax – www.equifax.com, Experian – www.experian.com, TransUnion – www.transunion.com)

If you receive spam or a phishing email about your taxes, do not click on the links or open any attachments, instead forward the email to phishing@irs.gov. Other tax scams or frauds can be reported according to the directions on this page: https://www.irs.gov/Individuals/How-Do-You-Report-Suspected-Tax-Fraud-Activity%3F.

Further Information

- Tax scam information from the IRS: https://www.irs.gov/uac/Tax-Scams-Consumer-Alerts.
- Security Awareness for Tax Payers guide by the IRS: https://www.irs.gov/pub/irs-pdf/p4524.pdf .
- Identity theft information from the FTC: https://www.identitytheft.gov/.

Provided By:

MS-ISAC MULTI-STATE Information Sharing & Analysis Center™

STOP | THINK CONNECT™