View Online

FS-ISAC | Security Tips Newsletter

March 2025 | Issue No. 19

Security is *Everyone's* Responsibility

'Tis the Tax Fraud Season

Summary

It's that time of year again and the possibility of phishing scams takes the usual tax-time anxiety to a whole new level as the Internal Revenue Service warns that fraudulent tax professionals are behind tax-related identity theft and financial harm.

These phishing and related scams are designed to trick the recipient into disclosing personal information such as passwords and bank account, credit card, and Social Security numbers, or into sending gift cards or wire transfers to the scammer.

US consumers and business owners should be extra vigilant, know the different phishing terms, and be aware of what the scams might look like:

Phishing/smishing – Phishing (emails) and smishing (SMS/texts) attempt to trick the recipient into providing sensitive information or downloading malware — i.e., malicious software — by clicking a link. Phishing emails are often sent to multiple email addresses at an organization to increase the chance someone will fall for the trick.

Spear phishing – This email phishing scam is more specific in that it targets potential victims individually and delivers a more effective email known as a "lure." These types of scams can be harder to identify because they are personalized, which makes the email seem more legitimate.

Whaling – Whaling attacks generally target leaders or other executives with access to large amounts of sensitive information at an organization or business. Whaling attacks can also target human resources or accounting office personnel.

Common Tax Fraud Methods

Fraudsters use a wide array of different themes in their campaigns, which often look like ordinary business communications. Train your personnel to spot these attempts and prevent the disclosure of credentials or other financial and business assets.

- Charity Impersonators
- COVID-19 Pandemic Scam
- Credits and Refund Misinformation
- Disaster Fraud
- Dishonest Tax Preparers
- Email and Text Message Impersonators
- Senior Fraud
- Social Media Bad Tax Advice and Scams
- Tax Debt Settlement and/or Relief Services
- Unclaimed Tax Refund
- Unemployment Claims Identity Theft
- Unexpected Tax Bill
- W-2 Form Fraud

Cloud-Based Schemes Aimed at Tax Preparers

The IRS and tax preparers continue to see attacks that exploit cloud-based applications.

- These cloud-related schemes trick their victims with realistic-looking phishing emails that contain links to websites that mimic cloud storage sites that look legitimate but are frauds. These scams are designed to collect the tax preparer's credentials, which the threat actor uses to access the real cloud storage site.
- Tax professionals using cloud-based applications are warned to use multi-factor authentication with information storage or run tax preparation software to help safeguard data. Multi-factor authentication requires at least two forms of identity, such as a password and a fingerprint, providing an extra layer of security.

Red Flags for Choosing a Tax Professional

"Ghost" preparers - The IRS requires that paid tax preparers sign returns. Unscrupulous "ghost" preparers, however, have the taxpayer sign and send the IRS their tax returns. These scammers often promise large refunds or charge low fees based on the refund amount. These red flags of unethical behavior can indicate fraud.

Valid ID for tax preparers - Taxpayers should always choose a tax preparer with a valid Preparer Tax Identification Number (PTIN). By law, anyone who is paid to prepare or assists in preparing federal tax returns must have a valid PTIN. Paid preparers must sign and include their PTIN on any tax return they prepare.

Safe Tax Preparers for Employers

Employers need to understand their payroll and employment tax responsibilities and choose a trustworthy tax prep service. Here are a couple of options:

- **A certified professional employer organization (CPEO).** Typically, these organizations are solely liable for paying the customer's employment taxes, filing returns, and making deposits and payments for the taxes reported related to wages and other compensation. They file employment tax returns and deposits and pay the combined tax liabilities of their customers using the CPEO's Employer Identification number. An employer enters into a service contract with a CPEO and then the CPEO submits Form 8973, Certified Professional Employer Organization/Customer Reporting Agreement to the IRS. Employers can find a CPEO on the Public Listings page of IRS.gov.
- **Reporting agent**. This is a payroll service provider that informs the IRS of its relationship with a client using Form 8655, Reporting Agent Authorization, which is signed by the client. Reporting

agents must deposit a client's taxes using the Electronic Federal Tax Payment System and can exchange information with the IRS on behalf of a client, such as to resolve an issue. They are also required to provide clients with a written statement reminding the employer that it, not the reporting agent, is ultimately responsible for the timely filing of returns and payment of taxes.

Reporting an IRS Impersonator

The IRS **doesn't initiate contact by email, text, phone, or social media** to request personal or financial information, and you can verify a suspicious message with the IRS. If you think it's a scam, report it.

- For potential email scams
- For letter or notice scams
- For potential social media message scams
- For potential text message scams
- For potential phone call scams
- For potential fax scams

If your Social Security number (SSN) or individual tax identification number (ITIN) was stolen, immediately report it to IdentityTheft.gov.

If You're a Victim?

Immediately change any passwords you might have revealed. Consider reporting the attack to IC3.govand the police, and file a report with the Federal Trade Commission.

Getting Help

If you identify suspicious activity involving your financial institution, contact them immediately.

TLP WHITE

12120 Sunset Hills Rd, Reston
VA 20190