suspicious link, filling out personal and financial information or downloading a malware file onto their computer.

Apr. 02, 2024

The Internal Revenue Service has kicked off its annual Dirty Dozen list with a warning for taxpayers to be aware of evolving phishing and smishing scams designed to steal sensitive taxpayer information.

With taxpayers continuing to be bombarded by email and text scams, the IRS and the Security Summit partners warned individuals and businesses to remain vigilant against these attacks. Fraudsters and identity thieves attempt to trick the recipient into clicking a suspicious link, filling out personal and financial information or downloading a malware file onto their computer.

"Scammers are relentless in their attempts to obtain sensitive financial and personal information, and impersonating the IRS remains a favorite tactic," said IRS

Commissioner Danny Werfel. “People can be anxious to get the latest information

designed to raise awareness and protect taxpayers and tax pros from common tax scams and schemes.

As a member of the Security Summit, the IRS has worked with state tax agencies and the nation’s tax industry for nine years to cooperatively implement a variety of internal security measures to protect taxpayers. The collaborative effort by the Summit partners also has focused on educating taxpayers about scams and fraudulent schemes throughout the year, which can lead to tax-related identity theft. Through initiatives like the Dirty Dozen and the Security Summit program, the IRS strives to protect taxpayers, businesses and the tax system from cyber criminals and deceptive activities that seek to extract information and money.

Phish or smish: Don’t take the bait

The IRS continues to see a barrage of email and text scams targeting taxpayers and others. These schemes frequently peak during tax season but they continue throughout the year. Taxpayers face a wide variety of these scams and schemes. And tax professionals, payroll providers and human resource departments remain favorite targets of email and text scams since they have sensitive personal and financial information. One common example remains the “new client” scam that can target tax pros and others.

That means taxpayers and tax professionals should be alert to fake communications posing as legitimate organizations in the tax and financial community, including the IRS and state tax agencies. These messages arrive in the form of unsolicited texts or emails to lure unsuspecting victims to provide valuable personal and financial information that can lead to identity theft. There are two main types:

- **Phishing:** An email sent by fraudsters claiming to come from the IRS. The email lures the victims into the scam with a variety of ruses such as enticing victims with

a phony tax refund or threatening them with false legal or criminal charges for tax

In some cases, phishing emails may appear to come from a legitimate sender or organization that has had their email account credentials stolen. Setting up two-factor or multi-factor authentication with their email provider can reduce the risk of individuals having their email account compromised.

Posing as a trusted organization, friend or family member remains a common way to target individuals and tax preparers for various scams. Individuals should verify the identity of the sender by using another communication method, for instance, calling a number they independently know to be accurate, not the number provided in the email or text.

The IRS initiates most contacts through regular mail and will never initiate contact with taxpayers by email, text or social media regarding a bill or tax refund.

What to do

Individuals should never respond to tax-related phishing or smishing or click on the URL link. Instead, report all unsolicited email – including the full email headers – claiming to be from the IRS or an IRS-related function to phishing@irs.gov. If someone experienced any monetary losses due to an IRS-related scam incident, they should report it to the Treasury Inspector General for Tax Administration (TIGTA), the Federal Trade Commission and the Internet Crime Complaint Center (IC3).

If a taxpayer receives an **email** claiming to be from the IRS that contains a request for personal information, taxes associated with a large investment, inheritance or lottery.

- Don't reply.

- Don’t open any attachments. They can contain malicious code that may infect the

If a taxpayer receives a **text** claiming to be from the IRS that contains a request for personal information, taxes associated with a large investment, inheritance or lottery.

- Don’t reply.
- Don’t open any attachments. They can contain malicious code that may infect the computer or mobile phone.
- Don’t click on any links. If a taxpayer clicked on links in a suspicious SMS and entered confidential information, they should visit Identity Theft Central.
- Report the message to 7726 (SPAM).
- Include both the Caller ID and the message body in an email and send to phishing@irs.gov. Copy the Caller ID from the message by pressing and holding on the body of the text message, then select Copy, paste into the email. If the taxpayer is unable to copy the Caller ID or message body, forward a screenshot of the message.
- Delete the original text.
- For more information see the IRS video on fake IRS-related text messages.

The Report phishing and online scams page at IRS.gov provides complete details. The Federal Communications Commission’s Smartphone Security Checker is a useful tool against mobile security threats.

Report fraud

As part of the Dirty Dozen awareness effort regarding tax schemes and unscrupulous tax return preparers, the IRS urges individuals to report those who promote abusive tax practices and tax preparers who intentionally file incorrect returns.

To report a tax scheme or a dishonest tax return preparer individuals should send a completed Form 14242, Report Suspected Abusive Tax Promotions or PreparersPDF,

(along with any supporting materials) via mail or fax to the IRS Lead Development

Taxpayers and tax professionals can also submit this information to the IRS Whistleblower Office, where they may be eligible for a reward. For details, refer to the sections on Abusive tax schemes and abusive tax return preparers.

Taxes