Hawthorne & Co.
Certified Public Accountants

IRS URGES CAUTION WITH EMAIL, SOCIAL MEDIA, AND PHONES AS PART OF "DIRTY DOZEN" SERIES

From the Internal Revenue Service – News Release: IR-2021-137

The Internal Revenue Service, on Tuesday, June 29, continues its "Dirty Dozen" scam series with a warning to taxpayers to watch out for unexpected schemes in the form of emails, text or social media messages and phone calls.

Unscrupulous individuals seek to obtain personal information for the purpose of tax-related identity theft. Whether through a telephone call, text message or email, the con artist tries to convince the recipient that they need to provide Social Security numbers, bank account or credit card information or passwords. The scam may also include sending links that once clicked on can download malicious software that collects, or "mines" personal data.

Often, criminals pose as someone the recipient knows or frequently interacts with, whether a social or family relationship or a business contact. They gather much of this information from social media. A person's contacts or 'friends' are used to bait the recipient into thinking they're dealing with someone they know.

Tax-related phishing scams persist

The IRS warns taxpayers, businesses and tax professionals to be alert for a continuing surge of fake emails, text messages, websites and social media attempts to steal personal information. These attacks tend to increase during tax season and remain a major cause of identity theft throughout the year.

Phishing scams target individuals with communications appearing to come from legitimate sources to collect victims' personal and financial data and potentially infect their devices by convincing the target to download malicious programs. Cybercriminals usually send these phishing communications by email but may also use text messages or social media posts or messaging.

These phishing schemes can be tricky and cleverly disguised to look like they're from the IRS or from others in the tax community. Taxpayers are reminded to continually watch out for emails and other scams posing as the IRS, like those promising a big refund, missing stimulus payment or even issuing a threat. People should not open attachments or click on links in those emails or text messages.

Phishing scams targeting tax professionals

As part of the Security Summit effort, the IRS warns tax professionals about phishing scams involving verification of Electronic Filing Identification Numbers (EFIN) and Centralized Authorization File (CAF) numbers. The agency has seen an increase in these kinds of scams, along with offers to buy and sell EFINs and CAFs.

Hawthorne & Co.
Certified Public Accountants

Tax professionals have reported receiving scam e-mails from the fictitious "IRS Tax E-Filing" and the IRS reminds tax professionals who receive those e-mails to not open any attachments or click any links. Rather, they should report the scam to the Treasury Inspector General for Tax Administration.

The IRS reminds tax professionals to protect themselves against the unauthorized use of an EFIN. Tax professionals must not transfer their EFIN or ETIN by sale, merger, loan, gift or otherwise to another entity.

Phishing – new client scams target tax pros

The "New Client" scam continues to be a prevalent form of phishing for tax pros. Here's an example in the form of an email: "I just moved here from Michigan. I have an urgent tax issue and I was hoping you could help," the email begins. "I hope you are taking on new clients."

The email says one attachment is an IRS notice and the other attachment is the prospective client's prior-year tax return. This scam has many variations so tax professionals should be wary and avoid opening attachments or clicking links when they don't know the e-mail sender.

Impersonator phone calls/vishing

Individuals should be wary of unexpected phone calls asking for personal financial information. The IRS has seen an increase in voice-related phishing, or 'vishing,' particularly from scams related to federal tax liens. For those receiving phone calls out of the blue, security experts recommend asking questions of the caller but not providing any personal information. If in doubt, hang up immediately.

During 2020, almost 400 vishing scams were reported, a 14% increase from the prior year. Of those vishing scams, 25% were scammers who tried to use fake tax lien information. The number of tax-lien related scams increased from 58 in 2019 to 104 in 2020, an increase of 79%. The IRS urges taxpayers to refrain from engaging potential scammers on the phone or online.

While both the IRS and the Federal Trade Commission have seen a decline in the number of reports of scammers claiming to be from the IRS telephoning potential victims, the agency urges taxpayers to be wary. (The IRS has seen a 43% decrease in the number of reports of calls from callers claiming to be from the IRS: 20,500 in 2020 compared to 36,000 in 2019. The FTC saw a 67% decline from 7,694 reports in 2019 to 2,571 in 2020.)

While the numbers may be on the decline, the IRS urges taxpayers to remain vigilant and to remember the following things about the IRS:

- The IRS generally first contacts people by mail - not by phone - about unpaid taxes.
- The IRS may attempt to reach individuals by telephone but will not insist on payment using an iTunes card, gift card, prepaid debit card, money order or wire transfer.
- The IRS will never request personal or financial information by e-mail, text or social media.

Recipients of these calls should hang up before giving out any information. If anyone receives an unexpected call from the IRS that they believe to be a scam, they can report it to the Treasury Inspector General for Tax Administration (TIGTA).

Social media scams continue

Taxpayers should be aware of social media scams, which frequently use events like COVID-19 to try to trick people. Social media enables unscrupulous individuals to lurk on accounts and extract personal information to use against the victim. These cons may send emails impersonating the victim's family, friends or co-workers.

Social media scams have also led to tax-related identity theft. The basic element of social media scams is convincing a potential victim that he or she is dealing with a person close to them that they trust via email, text or social media messaging.

Using personal information, a scammer may email a potential victim and include a link to something of interest to the recipient, but which contains malware intended to commit more crimes. Scammers also infiltrate their victim's emails and cell phones to go after their friends and family with fake emails that appear to be real, and text messages soliciting, for example, small donations to fake charities that are appealing to the victims.

Individuals should know that any of their information that is publicly shared on social media platforms can be collected and used against them. One way to circumvent these scams is to review privacy settings and limit data that is publicly shared.

Ransomware on the rise

Financial institutions should be aware of trends and indicators of ransomware, which is a form of malicious software ("malware") designed to block access to a computer system or data. Access is often blocked by encrypting data or programs on information technology (IT) systems to extort ransom payments from victims in exchange for decrypting the information and restoring victims' access to their systems or data. In some cases, in addition to the attack, the perpetrators threaten to publish sensitive files belonging to the victims, which can be individuals or business entities.

The U.S. Treasury Financial Crimes Enforcement Network (FINCEN), has noted that ransomware attacks continue to rise across various sectors, particularly across governmental entities as well as financial, educational and healthcare institutions. Ransomware attacks on small municipalities and healthcare organizations have increased, likely due to the victims' weaker cybersecurity controls, such as inadequate system backups and ineffective incident response capabilities.

Tactics

Cybercriminals using ransomware often resort to common tactics, such as wide-scale phishing and targeted spear-phishing campaigns that induce victims to download a malicious file or go to a malicious site. They may also exploit remote desktop protocol endpoints and software

vulnerabilities or deploy "drive-by" malware attacks that host malicious code on legitimate websites. Proactive prevention through effective cyber hygiene, cybersecurity controls and other best practices are often the best defense against ransomware.

Ransomware actors are increasingly engaging in selective targeting of larger enterprises to demand bigger payouts – commonly referred to as "big game hunting." Many cybercriminals are sharing resources to enhance the effectiveness of ransomware attacks, such as ransomware exploit-kits that come with ready-made malicious codes and tools. These kits can be purchased, although they are also offered free of charge.

Some ransomware groups are also forming partnerships to share advice, code, trends, techniques and illegally obtained information over shared platforms.

Ransomware criminals are also increasingly engaging in "double extortion schemes," which involve removing sensitive data from the targeted networks, encrypting the system files and demanding ransom.

The consequences of a ransomware attack can be severe and far-reaching, with losses of sensitive, proprietary, and critical information and loss of business functionality. The role of financial intermediaries in facilitating ransomware payments and ransomware attacks are a growing concern for the financial sector because of the critical role financial institutions play in the collection of ransom payments.

The IRS reminds taxpayers and tax professionals to keep abreast of news about fraud-related behavior. Report any instances of fraud immediately.

For more information visit Tax Fraud Alerts and Tax Scams – How to Report Them.