FULTON INDUSTRIAL BOULEVARD IMPROVEMENT DISTRICT

Public Safety Bulletin

Tax Scams

Every tax season, there are criminals trying to scam innocent people out of some of their money. Below you will find their top ten methods.

- **Phishing emails**

The IRS, other government agencies, and banks have been warning us about these emails for years, but they continue to be a problem. Some of these fraudulent emails will look like they are from the IRS or a bank and will ask you to visit their site and "update your account," according to the IRS. The page will look official, and criminals are hoping you'll enter your private information so they can use it to steal your identity, file a fake tax return in your name, or open new accounts without your knowledge.

There is a new twist on the theme this year. Fraudsters are sending emails pretending to be a professional association you might belong to, "like the state societies of opticians, or lawyers, or any other profession," Melanie Lauridsen, senior manager for tax policy and advocacy at the American Institute of CPAs (AICPA) told Business Insider.

Criminals will often use the official name of a professional association, or a very similar name, according to Lauridsen. The email will say that you need to login to update your information, such as licensure or registration info, and get you to enter other sensitive information. This leaves you vulnerable to identity theft or other fraud.

- **Phone calls from the "IRS"**

More and more of my clients have been getting random phone calls from scammers claiming to work for the IRS. The IRS will almost never make initial contact with you by phone.

"They like to target the elderly and recent immigrants, in particular, who may not be aware that the IRS will never call to demand immediate payment, nor contact taxpayers about taxes owed without first corresponding by mail or providing the taxpayer an opportunity to appeal a balance due."

These scammers have gotten sophisticated, according to the IRS. Now, they can spoof the local IRS Taxpayer Assistance Center (TAC) phone number to appear on your caller ID. If you doubt them, the scammers will tell you to look up the number.

Why do people fall for this? "Aggressive, high-pressure tactics enable schemes like this to work. Victims are threatened with arrest and other severe consequences if they don't make payment immediately. People react in a moment of fear and anxiety and do it."

The IRS does not do anything immediate— they have a process of warning letters, registered mail, and other paper information before they demand money.

- **Using your Social Security number to file a tax return and steal your refund**

Whether criminals have gotten your information from hacking, data breaches, or by using a phishing email that you fell for, if they have your social security number and other vital data about you, they can file a return in your name. “The scammers often get the refund put onto prepaid debit cards instead of being deposited in bank accounts because it's a lot harder to trace once the payment has been made. “We saw it at the height for our clients in 2017, but the number of incidents has been declining since then. If you can file early, this reduces your chances of having this scam pulled on you.

- **Fees based on your return amount**

"If a tax preparer says they can get you a $6,000 refund and will charge 10% of that for their fee, be suspicious," Lauridsen said. "Preparers should charge based on how much work it takes to do your return, not the amount they can get you as a refund. The IRS may quickly refund you the $6,000, but when they figure out that you don't have three extra children, huge donations to charities, or other sneaky tricks, the IRS will want that money back. “By then, that preparer will be long gone with your $600, while you'll be on the hook for paying back the IRS. No matter who you go to for tax preparation help, the amount of your refund shouldn't vary by much.

- **Pop-up tax preparers**

"With the in-person scam we often see fraudulent tax preparers. The preparer creates a business out of thin air and reports a loss on your tax return in order to inflate your refund." The best defense is to know who is preparing your return and to actually look over your return before filing it," Lindsey continued. "You don't have to understand every nuance of the tax law, but you should know if you had a side gig or not."

- **Harvesting information from hotspot or public WiFi networks**

Anyone can harvest your data on a public WiFi network. Don't file your taxes from Starbucks or McDonalds. Don't bank from there either. If you are a professional who works with sensitive data, use a VPN if you need to work while traveling. Then, when you log in from the airport or the coffee shop, you have safeguarded the information you are accessing.

- **Prize and trip email scams**

"You have not won anything, so do not click on that link," Lauridsen said. People get fooled every day, click on a link, and then the criminals can be inside your company's computer system, able to get to all kinds of files, from employee information to customer data. Stop and

think about it very carefully before you click on any link in an email — it might download malicious software that allows outsiders to access your private data.

- **Tricking businesses to release data**

"As the IRS has better filters in place to avoid identity theft, scammers have had to resort to going to businesses to try to get information to commit their various types of fraud." Lauridsen told us of one common scenario: "The 'CEO' of the company sends an email to the HR department, asking for sensitive data for all employees. "Not wanting to question the CEO, someone in HR sends out a spreadsheet with all the employees' complete information — social security numbers, bank account numbers, tax information, addresses, etc.," Lauridsen continued. "But really, it was a scammer having hacked or spoofed the CEO's email account."

If you get a suspicious request that is out of the ordinary, especially when it relates to personal data on employees, take the time to verify it through another channel. "You want to impress the boss, but be aware that scammers are able to make it look like they are using internal email accounts," Lauridsen said. It should be pretty easy to pick up the phone and check out the request. You may be the hero who averts a major data breach at your company.

- **Tax preparers getting hacked**

Because there are more robust identity theft filters in place, criminals are specifically targeting tax professionals with phishing emails posing as the IRS or software companies. The IRS warns that fraudsters are working to hack into CPA and tax preparer computers to steal their client information. All financial professionals need to have good cybersecurity installed and working to keep out intruders. In addition, there are programs that will automatically log you out if you step away from your computer for a few minutes — this is much safer than leaving the data open and available on your computer.

- **Fake tax bills through the mail**

Even though most IRS contact with taxpayers is through the mail, some mail might be a scam. "The IRS will generally contact taxpayers by regular mail before any other contact is made, and even that can be suspicious, because a growing scam involves fraudsters sending out phony tax bills through the mail on what looks like official IRS letterhead. "If you think you don't owe any tax or don't owe the amount shown on the bill, be careful not to fall for this scam. You should check with the IRS before paying any bill that looks suspicious."

Call police by dialing 911

3993 Aviation Circle NW, RM 024, Atlanta, GA 30336

Phone: (404) 328-5246 | www.boulevardcid.org