Tax and Other Identity Thefts

How to Prevent Them and What to Do When You Cannot

PLEASE NOTE THAT THE IRS WILL NEVER

- Call to demand immediate payment using a specific payment method such as a prepaid debit card, gift card or wire transfer.
- Generally, the IRS will first mail you a bill if you owe any taxes.
- Threaten to immediately bring in local police or other law-enforcement groups to have you arrested for not paying.
- Demand that you pay taxes without giving you the opportunity to question or appeal the amount they say you owe.
- Ask for credit or debit card numbers over the phone.

Business Fraud

Seena Gressin, attorney for the Division of Consumer and Business Education, FTC, writes, "tax identity thieves are already posting their "gone phishin' signs:" fake e-mails designed to get human resources officers to hand over their employees' personal information." Even the professionals get snookered. Cybercriminals send fake emails that look official. The so-called corporate office asks for the company's payroll or human resource office, requesting a quick review of the employees' W2 forms. This phishing variation is known as a "spoofing" email. It will contain, for example, the actual name of the company's chief executive officer. In this variation, the "CEO" sends an email to a company payroll office or human resource employee and requests a list of employees and information including SSNs. This is only one sneaky tactic. *But we're retired, so what should we be looking for?*

Personal Loss

Cybercriminals are after your social security number to file for a tax refund, get a job, or claim your child or a fake child as their dependent. The cybercriminals are using more and more sophisticated tactics to gain more and more of your information. If you receive an unexpected letter from the IRS, you may be alerted that someone else is using your number. Remember that the IRS will not initiate contact with you by sending emails, texts, or social media messages. If you get an email that claims to be from the IRS, do not reply or click on any links. Immediately report it to <phishing@irs.gov>.

File as early as possible to beat the crooks. If you get a letter from the IRS saying that more than one return was filed for you, someone is already using your social security number. That someone may have used your SS# to apply for a job. His or her employer may have submitted income you supposedly earned. The second filing—the one you sent in—makes it appear that you failed to report all your income. The IRS does not know that the employer's report was because someone used a stolen SS#. At this point, you are on the hook with the IRS.

Contact the IRS as soon as possible. A specialist will work with you to get your return filed correctly, get your refund as quickly as possible, and then protect your account. This specialist announcement all sounds clear cut. One individual has had his tax return usurped, not once, but twice. Some crook received his tax refund, and it was not refunded to him by the IRS until 11 months later. The next year, when he filed, the same nightmare happened again. The third year, he owed money, so he did not have problems. He and his wife had to appear at the IRS office with his affidavit of fraud, driver's license and passport and photos in April. Then they had to return again with the same documents in August to prove their identities again. He was perplexed when he had to repeat the procedures all over again with different officials. The IRS officials have issued him a pin number that must be submitted with his income tax forms. The IRS calls his account "compromised," a euphemism for what these criminals did to his identity and his refund. This year he is holding his breath. He sighs, "We will see in April." Thieves are slick. Once they have your social security number, you may expect to have problems periodically.

Protecting Your Identity

Be wary of giving your social security number to anyone, including the doctor's office who wants you to fill out forms in triplicate with your social security number glaring. Do not give them your social security number. They do not need it and cannot guarantee that their data system will not be breached.

The IRS saw an approximate 400 percent surge in phishing and malware incidents in the 2016 tax season. Some malware allows the crooks to see every keystroke you type and to access all your files. Scam emails are designed to trick taxpayers into thinking these are official communications from the IRS or others in the tax industry, including tax software companies. These phishing schemes can ask taxpayers about a wide range of topics. Emails can seek information related to refunds, filing status, confirming personal information, ordering transcripts and **verifying PIN information**. Do not fall into this trap.

Variations of these scams can be seen via text messages, and the communications are being reported in every section of the country. The IRS is aware of email phishing scams that appear to be from the IRS and include a link to a bogus web site intended to mirror the official IRS web site. These emails contain the direction "you are to update your IRS e-file immediately." The emails mention USAgov and IRSgov (without a dot between "IRS" and "gov"), though notably, not IRS.gov (with a dot). Don't get scammed. These emails are not from the IRS.

According to the Taxpayer Advocacy Panel (TAP), taxpayers are receiving emails that appear to be from TAP about a tax refund. These emails are a phishing scam, where unsolicited emails which seem to come from legitimate organizations — but are really from scammers — try to trick unsuspecting victims into providing personal and financial information. Do not respond or click the links in them. If you receive an email that appears to be from TAP regarding your personal tax information, please forward it to phishing@irs.gov and note that it seems to be a scam email phishing for your information.

TAP is a volunteer board that advises the IRS on systemic issues affecting taxpayers. It never requests, and does not have access to, any taxpayer's personal and financial information such as Social Security and PIN numbers or passwords and similar information for credit cards, banks or other financial institutions.

Recent scammers are also sending fake emails purporting to contain an IRS tax bill related to the Affordable Care Act.

What to Do Right Away

1. Call the companies where you know fraud occurred.
2. Place a fraud alert and get your credit report.
3. Report identity theft to the FTC.
4. File a report with your local police department.
5. Call the IRS Identity Protection Specialized Unit at 1-800-908-4490.
   a. Report the fraud
   b. Send a copy of the police report or an IRS Identity Theft affidavit form 14039 (PDF) and proof of your identity, such as a copy of your social security card, driver's license, or passport.
   c. Always record the dates that you made calls or sent letters.
   d. Keep copies all letters that you send.

What to Do Next

1. Take a deep breath and begin to repair the damage.
2. Close new accounts opened in your name.
3. Remove bogus charges from your accounts.
4. Correct your credit reports.
5. Consider adding an extended fraud alert or credit freeze or your credit reports.
   a. A fraud alert is free, but you must provide proof of your identity.
   b. A fraud alert on your credit report will make it more difficult for a thief to open more accounts. It lasts for 90 days, but it can be extended.
   c. Place a fraud alert by reporting that you are an identity fraud victim.
   d. Confirm that the credit company you call will contact the other two credit bureaus.
   e. Be sure that the credit companies have your correct contact data.

Transunion	**1-800-680-7289**
Experian	**1-888-397-3742**
Equifax	**1-888-766-0008**