AVOIDING FINANCIAL SCAMS CAN PREVENT ID THEFT

02/24/2021

Being confident about the security of your private information can be challenging in today's world. Help protect your identity with the following safe practices.

It can be unsettling for any taxpayer to be contacted by the Internal Revenue Service (IRS), but imagine receiving a telephone call and hearing this:

> *"This prerecorded message is to notify you that the IRS has found fraud and misconduct on your tax return. This needs to be resolved immediately, and it's very important that I hear from you as soon as possible or a legal action will be taken against you."*

Most people are quick to spot the call as a fake since the IRS doesn't threaten taxpayers by telephone, emails, or text messages, or issue arrest warrants. But any scam can work if you aren't paying close attention. Remember these guidelines:

- If something seems fishy, hit the brakes. Wait until your emotions have settled and research what's going on. Fraudsters use tight deadlines to try to force you into a rash decision.
- Never call back a number in a message asking for sensitive information, like in the example above. Don't follow a link in an unsolicited email, or text message either. Go to the website of the company, or organization, or call their main phone number and get in touch with them through direct channels.
- When in doubt, do an internet search for the company or organization involved, followed by the word "scam."
- If you think you've been a victim of identity theft, put a freeze on your credit files if you don't plan to borrow money soon, or place a fraud alert on your credit reports. The freeze prevents any new credit from being approved, but you can freeze and unfreeze your credit file for free. The fraud alert notifies lenders and creditors that they should take extra steps to verify your identity before extending credit.
- Contact one of the 3 credit bureaus to request a fraud alert or credit freeze:
    - Equifax at (800)525-6285
    - Experian at (888)397-3742
    - TransUnion (800)680-7289

6 COMMON SCAMS

Find out what to watch for and what to do if you think you're a victim of a financial fraud in these six common scams.

1. TECH SUPPORT SCAM

You may get a call alerting you to a problem with your computer, or a message may pop up on the screen saying your computer is infected with a virus. If you follow the instructions of the caller or the screen message, your computer may be taken hostage and your personal information stolen. You are then asked to pay a fee to restore access to your computer or data. What to do:

- Prevention is the best medicine. Don't click pop-up ads or attachments from unknown senders. Avoid clicking links in emails. Visit known websites by manually typing the URLs in a browser.

- Do not allow anyone to control your computer remotely and never give passwords and security codes to anyone on the phone.
- Hang up if you receive a tech support call, and don't respond to scare messages about your computer being infected. If you need help with your computer, go to your local computer or electronics store.
- Back up your data regularly. That way, you can reboot and regain control of your computer by cleaning your hard drive and reinstalling your operating system.
- Consider taking action to protect your accounts; including signing up for 2-factor authentication. And sign-up for highest levels of security offered.

2. TAX REFUND FRAUD

A criminal, having illegally obtained your Social Security number, files a fraudulent tax return in your name and collects a refund. When you submit your legitimate tax return, it is rejected because the IRS has already processed a return with your Social Security number. In some cases, you may receive a notice prior to filing your return that the IRS has received a suspicious return using your identity. What to do:

- File your return early, reducing the likelihood that a criminal would have previously filed a fraudulent return.
- If your return is rejected because of a duplicate filing under your Social Security number, you may submit Form 14039, Identity Theft Affidavit.
- Remember, the IRS will contact you through the US Postal Service, not a phone call.
- Do not return a call from someone claiming to be with the IRS.
- Visit Identity Theft Central for information about tax-related identity theft and data security protection from the IRS.
- Continue to pay your taxes and file your legitimate tax return, although you may have to submit a paper return rather than an electronic one. Attach Form 14039, Identity Theft Affidavit, when filing your return.

3. EMPLOYMENT OR HEALTH CARE FRAUD

A person could use your identity to obtain a job, or receive health care services. You may get a letter from the IRS after filing your taxes saying that you appear to have underreported your income, or in the health care version of the scheme, you get a bill for medical exams, procedures, and prescription drugs that you never received. The pandemic has provided scammers with opportunities for fraud, and the Office of the Inspector General in Health & Human Services has issued a fraud alert connected to COVID-19 related health care scams. What to do:

- If you suspect you are a victim of taxpayer identity theft, immediately contact the IRS and file Form 14039, Identity Theft Affidavit
- Never surrender Social Security, Medicare, or health insurance numbers to anyone you don't know and trust.
- If you believe someone has signed up for health insurance in your name, call the *Health Insurance Marketplace* call center at 800-318-2596, and explain the situation.
- If it's Medicare-related, file a complaint with the Office of the Inspector General in Health & Human Services.
- Review the Medical Identity Theft checklist.

4. UNEMPLOYMENT BENEFITS SCAM

Scammers who apply for unemployment benefits in your name could prevent your legitimate claim from going through—while they collect the benefits you're entitled to.

This scam became more prevalent in 2020 as unemployment benefits were temporarily expanded due to COVID-19. If you have a job, your employer may alert you to a fraudulent claim in your name or you may find out when the unemployment office sends a letter about a recent claim. What to do:

- Notify the unemployment office in your state about the fraudulent claim.
- Report the crime and start a recovery plan on https://identitytheft.gov/
- Be sure to review the identity theft page maintained by your state as well for more potential steps.
- File a police report if possible.
- Freeze your credit or put a fraud alert on your credit reports.

5. CREDIT CARD FRAUD

Someone using your identity signs up for a credit card and racks up large charges. A crook who obtains a new card could use it extensively before being discovered. Sometimes, a stolen identity is used to obtain personal loans or open unauthorized financial accounts. You will likely learn about this when bills are not paid and you are contacted by collection agencies looking for payment. You may notice either you are not getting any postal mail (due to address fraud or theft), or you start receiving confirmation or decline letters for credit cards or loans that you did not initiate. What to do:

- Report the crime and start a recovery plan on https://identitytheft.gov/
- File a police report.
- Freeze your credit, or put a fraud alert on your credit reports.
- Sign up for alerts from your bank or credit card issuer to stay on top of your legitimate accounts.

6. FAKE CHARITIES

You are solicited by email, phone, or in person to contribute to an organization that sounds like a good cause but is actually a scam. Such schemes may be general in nature, often using a name very similar to a well-known charity, or they may be more targeted, attempting to prey on people who are victims of a natural disaster or known to have a personal interest in a particular disease or social cause. These days, charity scams are also being circulated through social media posts on sites like Facebook, Twitter, and LinkedIn. What to do:

- Before contributing, research the charity through the Better Business Bureau's (BBB).
- If you suspect you have been a victim of charity fraud, file a complaint on https://identitytheft.gov/

IN SUMMARY

- Enroll in additional security features like 2-factor authentication, and secure your mobile phone, and email accounts.
- Be wary of calls or emails threatening legal action or account closures. Don't trust calls from individuals claiming to represent technical support, the IRS, or your financial institutions.
- File your tax return as early as possible.