What to Do If Someone Stole Your Social Security Number

In a perfect world your personal information, like your Social Security number, is confidential and secure. But accidents happen and data breaches can occur at any time, leaving your identity information compromised and at risk of fraud or theft.

In December, the Social Security numbers of over 35,000 PayPal users were stolen in a cyberattack, leaving critical personal information in the hands of cyber hackers and thieves.

These sorts of hacks happen frequently, and in their aftermath, identity theft can have a long-lasting impact on a person's credit score.

But just because it's a constant threat doesn't mean you can't take steps to protect yourself. Here's how to keep your personal information safe and what to do if your Social Security number has been stolen.

How does your personal information get stolen?

Theft happens everywhere, all the time. People will steal wallets and bags or go through mail in search of personal bank or credit card information. The Social Security Administration warns that people rummaging through trash outside of homes or businesses in search of critical information is another way identity theft takes place, along with people buying personal information from insider sources. There's also the risk of receiving phone calls, texts or emails from seemingly official sources who are actually fraudsters looking to trick you into revealing information.

Cyberattacks happen when hackers take to online accounts with combinations of usernames and passwords that are often stolen in previous data breaches and used to break into as many accounts as they can. That strategy is reason enough to diversify your passwords and implement two-factor authentication whenever possible.

If you think that you have been a victim of a Social Security theft, what should you do?

First, if you think your Social Security number has been stolen, know that the administration itself can't do much if someone uses your stolen information to, for example, open up a line of credit or get a job.

Head to the Federal Trade Commission's IdentityTheft.gov and fill out a form to receive a personal recovery plan. This plan walks you through all you need to know about protecting yourself from fraud and recovering your identity. You can also call 877-438-4337.

Contact the Internal Revenue Service if your Social Security number has been stolen to prevent the thief from using your number to file a tax return and receive your tax refund or to prevent them from using your number for a job. If a thief uses your Social Security number to get a job, owed taxes may show up on your record. Visit the IRS's Identity Theft Central to dispute these claims, get help and clear up any issues you have.

File an online complaint with the Internet Crime Complaint Center, which monitors cybercrime complaints to combat internet crime. It's also advisable to check your credit report every so often to quash any fishy behavior as it happens. Visit www.annualcreditreport.com to receive a free credit report.

Contact the Social Security Administration if you think your Social Security number has been compromised and the administration can help review your statements.

Do you need a new Social Security number?

If you have done all the steps that the Social Security Administration recommends and your Social Security number is no longer being used by someone other than yourself, then you don't need to apply for a new SSN. If you've taken all of the necessary steps and still find that your number is being used, you can apply for a new one.

But the administration doesn't make it easy to get a new SSN. You'll need proof that your number continues to be used by someone other than yourself. The administration said if you lost your card or think someone stole your number but have no evidence of someone else using it, you won't be able to receive a new one.

What can you do in the future to help prevent identity theft?

Sometimes, like with the PayPal breach, there is little you can do to keep your information safe. But there are steps you can take to limit your risk.

Don't carry around your Social Security card in your wallet. Instead, store it in a safe place in your home. Try to memorize your SSN so you don't have to take your card out every time you're filling out a

document that requires it. If you have to provide your number over the phone, make sure you're far away from other people who could possibly hear it.

Employers and landlords often request documents to be sent electronically through email. If you have to provide your Social Security number or other personal documents by email, try encrypting the document with a password or providing your SSN separately in a phone call.

Your employer will need your Social Security number to run a background check. But you should be skeptical of any job posting that requires you to enter personal information at the outset of an application. Unless you are starting a new position and have an offer in hand, you should not provide your SSN to a recruiter.

Finally, always check your bank statements and credit statements regularly to address any issues as soon as they pop up. Enable two-factor authentication on your passwords to protect your private information on websites and apps. And verify the source of your notices -- whether they're phone calls or emails. The Social Security Administration said in general it will only call you if you requested a call. If you believe you've received a scam call or email, don't give the person any personal information.