How to Protect Yourself Against Identity Theft

Massive computer hacks and data breaches are now common occurrences — an unfortunate consequence of living in a digital world. Once identity thieves have your information, they can use it to gain access to your bank and credit card accounts, make unauthorized transactions in your name, and subsequently ruin your credit.

Now more than ever, it's important to safeguard yourself against identity theft. Here are some steps you can take to protect your personal and financial information.

Check yourself out

It's important to review your credit report at least once a year and make sure that all the information in it is correct. Every consumer is entitled to a free credit report every 12 months from each of the three reporting agencies: Equifax, Experian, and TransUnion. Besides the annual report, you may be entitled to an additional free report under certain circumstances. Visit annualcreditreport.com for more information.

If you find an error in your credit report, contact the appropriate credit reporting agency to let it know that you are disputing information on your report. The agency usually must investigate the dispute within 30 days of receiving it. Once the investigation is complete, the agency must provide you with a written result of its investigation and remove/correct any errors. You can generally file your dispute with the agency either online or by mail. However, it may be more helpful to dispute the error in writing with supportive documents, preferably by certified mail. That way you'll have a paper trail to rely on if the investigation does not resolve the disputed error. If you believe that the error is the result of identity theft, you can also file a complaint with the Federal Trade Commission at identitytheft.gov.

In addition to checking out your credit report, you should regularly review your bank and debit/credit card accounts for suspicious charges or account activity. If you discover signs of unauthorized transactions, contact the appropriate financial institution as soon as possible — early notification not only can stop the identity thief but may limit your financial liability.

As you monitor your credit report and financial accounts, keep an eye out for the following possible signs of identity theft:

- Incorrect personal and account information on your credit report, including suspicious credit inquiries
- Money that is missing from your bank account, no matter how small the amount
- Missing bills or other mail from financial institutions and credit card companies

Consider a fraud alert and/or security freeze if necessary

If you discover that your personal and/or financial information has been exposed to identity theft, you should consider placing a fraud alert and/or security freeze on your credit report.

A fraud alert requires creditors to take extra steps to verify your identity before extending any existing credit or issuing new credit in your name. A fraud alert lasts for 90 days and can be renewed once it expires (an extended fraud alert that lasts for seven years is also available). To request a fraud alert, you only have to contact one of the three major credit reporting agencies, and the information will be passed along to the other two.

A security freeze prevents new credit and accounts from being opened in your name. Once you obtain a security freeze, creditors won't be allowed to access your credit report and therefore cannot offer new credit. This helps prevent identity thieves from applying for credit or opening fraudulent accounts in your name. Keep in mind that if you want to apply for credit with a new financial institution in the future, open a new bank account, and even apply for a job or rent an apartment, you will need to "unlock" or "thaw" the security freeze. In addition, you must contact each credit reporting agency separately to place a security freeze on your credit report.

Maintain strong passwords

Most of us have a large amount of personal and financial information that's readily accessible through the Internet, in most cases protected by nothing more than a username and password.

A strong password should be at least eight characters long, using a combination of lower-case letters, upper-case letters, numbers, and symbols or a random phrase. Avoid dictionary words and personal information such as your name and address. Also create a separate and unique password for each account or website you use, and try to change passwords frequently.

If you have trouble keeping track of all your password information or you want an extra level of password protection, consider using password management software. Password manager programs generate strong, unique passwords that you control through a single master password.

Stay one step ahead

The best way to avoid becoming the victim of identity theft is to stay one step ahead of the identity thieves. Here are some extra precautions you can take to help protect your sensitive data:

Consider using two-step authentication. Two-step authentication, which involves using a text or email code along with your password, provides another layer of protection for your information.

Think twice before clicking. Beware of emails containing links or asking for personal information. Never click on a link in an email or text unless you know the sender and have a clear idea where the link will take you.

Search with purpose. Typing one word into a search engine to reach a particular website is easy, but it sometimes isn't enough to reach the site you are actually looking for. Scam websites may look nearly identical to the one you are searching for. Pay attention to the URL, which will be intentionally misspelled or shortened to trick you.

Be careful when you shop. When shopping online, look for the secure lock symbol in the address bar and the letters https: (as opposed to http:) in the URL. Avoid using public Wi-Fi networks for shopping, as they lack secure connections.

Beware of robocalls. Criminals often use robocalls to collect consumers' personal information and/or conduct various scams. Newer "spoofing" technology displays fake numbers to make it look as though calls are local, rather than coming from overseas. Don't answer calls when you don't recognize the phone number. If you mistakenly pick up an unwanted robocall, just hang up.

Be on the lookout for tax-related identity theft. Tax-related identity theft occurs when someone uses your Social Security number to claim a fraudulent tax refund. You may not even realize you've been the victim of identity theft until you file your tax return and discover that a return has already been filed using your Social Security number, or the IRS sends you a letter indicating it has identified a suspicious return using your Social Security number. If you believe that you are the victim of tax-related identity theft, contact the Internal Revenue Service at irs.gov.

Because of the amount of paperwork and steps involved, fixing a credit report error can be a time-consuming and emotionally draining process. If at any time you believe your credit reporting rights have been violated, you can file a complaint with the Consumer Financial Protection Bureau (CFPB) at consumerfinance.gov.

Remember that the IRS will never contact you by email to request personal or financial information. This includes any type of electronic communication, such as text messages and social media. If you get an email claiming to be from the IRS, don't respond or click any links; instead, forward it to phishing@irs.gov.