GEN Y PLANNING®
FINANCIAL PLANNING FOR MY GENERATION

Protect Your Money: Your Guide to Preventing Identity Theft

No One Is Immune to Identity Theft, But You Can Lower Your Risk and Keep Yourself Safe

Identity theft is unfortunately common, and anyone can be a victim. Nearly a quarter of people over the age of 16 in the U.S. experienced identity theft in their lifetime, according to the Bureau of Justice Statistics' 2021 report, "Victims of Identity Theft."

The bad news is there's not a ton you can do to stop it from happening. But here's the good news: you can take actions every day to lower your risk of having your financial information ending up in the wrong hands. And taking quick action if you do notice something unusual with one of your accounts can prevent further damage.

With scams growing more sophisticated, it's essential to understand how to lower your risk of becoming an identity theft victim, and what actions to take if it happens to you.

How Identity Theft Can Happen

Identity theft can start with someone stealing your physical property, like a credit card or bank statement. But it can also happen when you click on a link in an email, give your information out over the phone, or even shop online. Major retailers, credit bureaus, healthcare providers, and other businesses have experienced data breaches where their customers' personal information was compromised.

Your information can also be stolen through skimming, which is when a device that logs information is attached to an ATM or payment terminal. Skimming can also happen digitally, when hackers steal stored customer information, such as credit card numbers, from retailers' websites.

Scammers can also send fake emails (called "phishing") or texts (called "smishing") asking you to click a link or submit personal information. You may receive a call from a scammer claiming to be your bank, or even someone claiming to be a loved one asking for money.

Some of these scams are so subtle, you may not notice anything is wrong until you receive notice of a data breach, or until you see an odd charge on a credit card.

How You Can Lower Your Risk

Protect physical sources of information

Carry your wallet in your front pocket. If you wear a purse, choose one with a zipper closure, and don't hang your purse from the back of your chair at a restaurant or leave it unattended. Keep your Social Security card at home in a safe location, and if you have any open credit cards you don't use often, leave them at home, too. You can even lock rarely used credit cards in your bank's app, and unlock them when needed. Shred any documents with your personal information on them before throwing them away. Lock your phone so it requires a passcode, your face, or your fingerprint to unlock.

Keep passwords secure

Ideally, you won't reuse the same passwords for different logins. That's a lot to memorize, but a password manager can help by securely storing your passwords. Creating strong passwords is easy with a password generator. Some tools, like LastPass and 1Password, do both – creating randomized passwords and storing them safely. You can also use these tools to share passwords with other trusted people.

Be cautious when using public Wi-Fi

Don't conduct any financial business, like paying bills or checking bank balances, on public Wi-Fi. Use your phone's data plan, or wait until you're home and can use your own password-protected Wi-Fi. Using a Virtual Private Network, or VPN, on public Wi-Fi can help keep your information more secure because it hides your browsing activity from others using the same Wi-Fi network.

Watch out for nosy strangers

If people are near enough to read your phone or computer screen, or a paper form you're filling out, they can steal any personal information they see.

Check your credit card and bank statements frequently

Look for charges or withdrawals you don't remember making. They can even be for just a few dollars. Report suspicious activity to your bank immediately. In the case of fraud on a credit card, most banks will waive the charges and send you a new card with a new account number (be sure to change the number on any bills or subscriptions that are automatically charged!). But if money is taken out of your bank account, it can take a few weeks for it to be refunded. Plus, the longer you wait to report fraud from a debit card or checking account, the more you'll be responsible for the stolen funds.

Use digital wallets and virtual card numbers

When you make a purchase and pay using either of these technologies, the store receives a random code instead of your actual credit card number. This helps keep your information safe in case a retailer experiences a data breach.

Check your credit reports for errors or accounts you didn't open

Mistakes and fraud can negatively affect your credit score, so if you notice something unusual, dispute it with the relevant credit bureaus. You can access your credit reports from Experian, Equifax, and TransUnion weekly for free at annualcreditreport.com. You can also request to freeze your credit through the credit bureaus, which will prevent others from opening new accounts in your name. You can unfreeze it temporarily to apply for a credit card or loan, and then freeze it again.

Use digital wallets and virtual card numbers

When you make a purchase and pay using either of these technologies, the store receives a random code instead of your actual credit card number. This helps keep your information safe in case a retailer experiences a data breach.

Beware of suspicious communications

If you get a weird email, text, or phone call, assume it's a scam. If someone's claiming to be from a certain company and asks for your information, hang up the phone or don't reply to the email or text. Look up that company's customer service number on their website and call to see if they were actually trying to get in touch with you.

Take actions if you were part of a data breach

You'll receive a letter from the affected company. Check your credit reports, and take advantage if they offer free access to credit monitoring services. If you were part of a data breach, we highly recommend freezing your credit.

Should You Use a Credit Monitoring Service?

Credit monitoring services can be helpful when you know you've been the victim of identity theft, you don't want to freeze your credit, or you don't want to make the effort to monitor your credit on your own. But these services can cost a few hundred dollars per year, and much of what they do, you can do yourself for free.

If you're considering a credit monitoring service, look into what they offer for the price, when and how you can cancel your service, and your rights if they don't protect you. Some offer a VPN or antivirus protection, which could be worth it if you were planning on paying for those anyway. Some also provide insurance that will cover the costs of restoring your identity. Make sure to find a credit monitoring service that keeps an eye on activity in all three of the main credit bureaus.

It's important to know the limits of these services. They can't prevent identity theft from happening. You'll still get phishing emails and weird texts, your credit card number might get stolen, and someone may try to open an account in your name. They're merely a way to be alerted to suspicious activity. Once you get that alert, you need to take actions to correct the issue.

Your credit card company also keeps an eye on your account for unusual spending patterns, and will alert you when they occur. So, again, credit monitoring services may not provide much beyond what you already have in place.

Credit Monitoring Service Options

There are many credit monitoring services available. Here are a few:

Aura

Cost: $12.99 to $32.99 per month. There are discounts for paying annually.

Aura offers plans for individuals, couples, and families. It monitors your presence online, as well as your accounts for possible breaches. You can also get a VPN, password manager, anti-virus protection, and more. Family plans offer parental controls, too.

LifeLock

Cost: $8.33 to $40 per month. There are discounts for paying annually.

LifeLock has a variety of plans to choose from, offering features such as reimbursement if you're a victim of a scam or identity theft. You'll also get alerts when there's suspicious activity on one of your accounts, along with social media monitoring. Some plans offer a VPN.

IdentityIQ

Cost: $8.49 to $31.49 per month. There are discounts for paying annually.

IdentityIQ offers credit monitoring, credit score change alerts, reimbursement for stolen funds, and even some coverage if you need to hire a lawyer. You can add a VPN and antivirus protection for an additional cost.

Not 'If,' But 'When'

It's not comforting to know that identity theft is something you can never fully prevent. But many of the same things you do to keep track of your finances, like reviewing credit card statements and periodically checking your credit reports, are also ways to keep your information secure.

At Gen Y Planning, the security of our clients' information is an essential part of managing our business. That's why we use many of the tools we recommend to you — a VPN, multi-factor authentication and a password manager. Treating your own personal information with care can make a huge difference in your level of risk.