How to Prevent Identity Theft

Our personal data is everywhere, and providing information like passwords and account numbers to access online accounts is something many of us do on a daily basis. Unfortunately, whenever we supply our PII, we are taking some level of risk that a criminal could steal and misuse it. But there are ways to reduce the likelihood of identity theft, and many of these strategies are simple and free.

The best way to help prevent identity theft is to sign up for an identity theft protection service. Although an identity theft protection service can't prevent identity theft, it can alert you promptly when it happens to limit the damage and help you recover. Identity theft protection can help safeguard your personal information for a monthly or annual fee. Subscriptions can include monitoring of credit reports, financial accounts, medical information, social media activity, the dark web, and more. Identity theft protection companies also provide recovery services if your information is compromised. Some offer identity theft coverage of up to $1 million and access to attorneys or private investigators to help you restore your credit and reputation. Most also give you a dashboard to view notifications and contact customer service if fraudulent activity occurs.

Besides subscribing to an identity theft protection service, there are other ways to help prevent identity theft. These include:

1. Freeze your credit.
When you freeze your credit file, no one can look at or request your credit report. Therefore, no one (including you) can open an account, apply for a loan, or get a new credit card while your credit is frozen. To freeze your credit, you must contact each of the three credit reporting agencies: Experian, Equifax, and TransUnion. The credit bureaus provide online, telephone, or mail-in options for freezing your account. Upon doing so, they will provide you with a PIN or passcode you can later use if you temporarily lift or stop the credit freeze. Credit freezes are free and won't impact your credit score.

Parents should seriously consider freezing their children's credit files. A 2021 study by Javelin Strategy & Research found that child identity fraud costs U.S. families nearly $1 billion annually. About 1 in 50 U.S. children were victims of ID fraud, and 1 in 45 had personal information that was exposed in a data breach. This can cost the average family more than $1,000.

"It's a good idea to put a freeze on children's credit files and to monitor those files as they approach their teen years," says Robert Douglas, an information and security consultant and certified identity theft risk management specialist. "There are plenty of horror stories out there of people finding out that their child's credit worthiness has been harmed at a critical point when they need a good, clean record like when applying for a student loan."

2. Collect mail daily.
Some of the ways that criminals can steal your identity are decidedly low-tech. For example, they can simply take bank or credit card statements, utility bills, health care or tax forms, or pre-approved credit card offers out of your mailbox. Thieves also can reroute your mail by submitting change-of-address requests in your name, so keep track of expected mail that doesn't arrive. In addition, put your mail on hold while you're away.

3. Review credit card and bank statements regularly.
It's important to regularly review your credit card and bank statements, because someone with your credit card number or bank account information could make small charges to see if they can get away with it. These transactions can easily slip through the cracks without you or your financial institution

noticing them. Know your statement cycles and follow up with credit card companies and financial institutions if you don't receive statements on time. Credit card fraud is the most common type of identity theft, based on FTC Consumer Sentinel Network statistics.

4. Shred documents containing personal information before disposing of them.
Dumpster diving might sound like an old-fashioned way of stealing personal information, given the influx of phishing scams and online data breaches, but criminals still do it. While some people might be looking for valuables or furniture, others are looking to steal your data.

Keep a few months of credit card and bank statements, utility bills, IRS correspondence, and other documents containing PII in a secure location like a safe. Shred the rest. Bagdasarian says he keeps his last three bank statements somewhere safe, replacing them with new ones every month.

5. Create different passwords for your accounts
A secure password is long, complex, and unique, according to the FTC. Create different passwords for various accounts. Avoid using information related to your identity, such as the last four digits of your Social Security number, your birthday, your initials, or parts of your name.

The FBI and National Institute of Standards and Technology recommends creating passwords with at least 15 characters because these are more difficult for a computer program or hacker to crack. As for security questions, the FTC advises selecting questions that only you can answer, instead of information that could be available online like your ZIP code, birth place or mother’s maiden name. Also, avoid giving generic responses, such as “chocolate,” as your favorite dessert.

6. Review credit reports annually
Requesting your credit reports from Equifax, TransUnion, and Experian is free, and you should do so annually. Accessing your credit reports won't lower your credit score, and you can easily request them online. Also, the bureaus provide tools to help you monitor your credit, such as alerts to notify you of key changes. Ideally, pull your report from the bureaus at different times throughout the year so you are continually monitoring activity. You can also request free annual credit reports at AnnualCreditReport.com.

7. Install antivirus software
Antivirus software can prevent hackers from accessing information on your computer and mobile devices. The FTC says you might be a victim of malware, which includes viruses, spyware, and other unwanted software, if your computer:

- Slows down, crashes, or displays error messages
- Fails to shut down or restart
- Delivers pop-ups or other unwanted ads
- Sends you to web pages you didn't search for
- Shows new, unexpected toolbars
- Changes your default web browser
- Drains its battery quickly

Because criminals can more easily hack outdated software, keep your antivirus software current or set it to update itself automatically. For more information, see How Does Antivirus Software Work?

8. Enable two-factor authentication on devices and accounts
According to a 2017 Data Breach Investigations Report from Verizon, 81% of hacking-related breaches start with a stolen or compromised password. Two-factor authentication (2FA) is an extra layer of

password security. It’s based on your knowledge of something like a PIN or password, a possession like a smartphone or other device, and a biometric characteristic like your fingerprint or voiceprint. 2FA requires more than one of these identifiers to unlock an account. Thus, if your password is stolen, a criminal still can't get into your account without your smartphone, voiceprint, or fingerprint. An example of 2FA at work is when you sign into an account with a password and then receive a text with a code you must supply to get into the account. You should set up 2FA for email, social media accounts, bank accounts, and credit cards.

9. Wipe electronics before donating
When you delete files from computers and other electronic devices like tablets, those files aren't really gone; pieces of them remain and can be reassembled with a data recovery program until they're overwritten with new data. This can be accomplished with overwriting software that wipes hardware or transfers data from your old computer to a new one.

10. Opt out of prescreened credit card offers
Credit card companies often send pre-screened offers to open new accounts, and criminals can intercept these mailed or emailed offers and open accounts in your name. Shred these offers rather than throwing them in the trash. Your credit report doesn't show pre-screening that companies perform to give you these offers, so you might not realize that an offer has been stolen from your mail or email.

The safest way to avoid identity theft exposure from pre-screened credit card offers is to opt out of receiving them for five years or permanently through optoutprescreen.com, which is the official consumer credit reporting industry website.

Where Could an Identity Thief Access Your Personal Information?

Consumer.gov warns that criminals can access your personal information a number of ways. These include:

- Hacking
- Stealing mail to get account numbers or your Social Security number
- Posing as an impostor and requesting information via email
- Stealing account numbers from businesses, credit card companies, and medical offices
- Simply taking your wallet or purse to access credit cards, your driver’s license, and other personal data

How to File a Police Report for Identity Theft

You can report identity theft to the FTC, which will help prove to businesses that someone stole your identity. You also have the right to place a one- or seven-year fraud alert on your credit report, request that fraudulent information is removed from your report, and stop debt collectors from contacting you.

You might want to file a police report for identity theft if you know the person who committed the crime, or if you find out the thief used your name or information during a police interaction, such as pretending to be you upon arrest. Credit card companies or financial institutions might request that you file a police report if you claim identity theft and ask them to investigate the case, remove the fraudulent activity from your account or cover the cost of lost funds.