Identity Theft: What It Is, How to Prevent It, Warning Signs and Tips


nerdwallet.com/article/finance/how-to-prevent-identity-theft

Identity theft is when someone uses your personal data — your name, Social Security number, birthdate, etc. — to impersonate you, typically using that information to steal from you. The Federal Trade Commission received more than 1.1 million complaints of identity theft through its IdentityTheft.gov website in 2022.

Here's what you need to know to reduce chances you'll be a target, spot warning signs and take quick action to minimize damage.

What is identity theft?

Identity theft happens when someone uses your sensitive data to pose as you or steal from you. Identity thieves may drain your bank and investment accounts, open new credit lines, get utility service, steal your tax refund, use your insurance information to get medical treatments, or give police your name and address when they are arrested.

Frequent data breaches mean your information may already be exposed. In this new reality, it's smart to take steps to prevent malicious actors from using your personal information and ruining your financial life.

7 types of identity theft and the warning signs

Once a criminal has your info, here are common ways it may be exploited:

1. Credit identity theft

Credit identity theft happens when a criminal uses your personal information, such as birthdate and Social Security number, to apply for a new credit line.

Warning signs: You might see an unexpected change in your credit scores or an account you don't recognize on your credit reports. You may get debt collection notices or a court judgment against you. The best way to prevent it is to freeze your credit.

2. Child identity theft

Criminals steal a child's identity and apply for credit in that child's name. Often it is not discovered until the victim applies for college loans or other credit.

Warning signs: If your child is getting offers of credit cards or phone calls about late payments or debt collections, investigate. You can freeze your child's credit to prevent it.

3. Synthetic identity theft

Synthetic identity theft is when criminals use a patchwork of identity details to construct a fictitious consumer, using a Social Security number — often one of a minor child or one that is simply made up — that is not yet in the credit bureaus' database and combining it with a name and address. They then apply for loans and credit cards, often making payments for years as the credit limits grow. Then comes a "bust out," when cards are maxed out and the criminals disappear.

Warning signs: If you try to freeze your child's credit and discover their Social Security number is already in use. Often it is not discovered until the child is applying for student loans. It is not always preventable, because sometimes criminals make up and use a Social Security number even before it's assigned.

4. Taxpayer identity theft

Sometimes fraudsters use a Social Security number to file a tax return and steal your tax refund or tax credit.

Warning signs: You may be unable to e-file because someone else has already filed under that Social Security number, you get an IRS notice or letter referencing some activity you knew nothing about or IRS records suggest you worked for an employer that you did not. Filing early can help you beat criminals to filing in your name, and some states offer six-digit identity protection PINs (after a rigorous verification) with additional security.

5. Medical identity theft

Using someone else's identity to get health care services is medical identity theft. It's particularly dangerous because it can result in medical histories being mixed, giving doctors and hospitals wrong information as they are making health care decisions.

Warning signs: Claims or payments on your insurance explanation of benefits that you do not recognize can suggest that someone is using your health care benefits. If you've fallen victim, you'll need to both report it to your insurance company and inform your health care team to be sure information in your health care records is actually yours.

6. Account takeover

Criminals use personal data to access your financial accounts, then change passwords or addresses so that you no longer have access.

Warning signs: An email, letter or text from your financial institution that refers to an action (like a password or email change) or transaction you don't recognize.

7. Criminal identity theft

Criminal identity theft occurs when someone gives law authorities someone else's name and address during an arrest or investigation. This is often done with false identification, such as a fake driver's license.

Warning signs: You may be detained by a police officer for reasons that are unclear to you, or be denied employment or a promotion because of something found in a background check.

11 ways to prevent identity theft

You're unlikely to find a fail-safe way to prevent identity theft, and monitoring services only let you know after something has gone wrong. But there are 11 things you can do to make it much harder for identity thieves.

1. Freeze your credit

Freezing your credit with all three major credit bureaus — Equifax, Experian and TransUnion — restricts access to your records so new credit files cannot be opened. It's free to freeze your credit and unfreeze when you want to open an account, and it provides the best protection against an identity thief using your data to open a new account.

2. Safeguard your Social Security number

Your Social Security number is the master key to your personal data. Guard it as best you can. When you are asked for your number, ask why it is needed and how it will be protected. Don't carry your card with you. Securely store or shred paperwork containing your Social Security number.

3. Be alert to phishing and spoofing

Scammers can make phone calls appear to come from government entities or businesses, and emails that appear to be legitimate may be attempts to steal your information. Initiate a callback or return email yourself, working from a known entity such as the official website, rather than responding to a call or email. And be wary of attachments — many contain malware.

4. Use strong passwords and add an authentication step

Use a password manager to create and store complex, unique passwords for your accounts. Don’t reuse passwords. Adding an authenticator app can reduce your risk. Don’t rely on security questions to keep your accounts safe; your mother’s maiden name and your pet’s name aren’t hard to find. Think carefully about what you post on social media so you don't give away key data or clues about how you answer security questions.

5. Use alerts

Many financial institutions will text or email when transactions are made on your accounts. Sign up so that you know when and where your credit cards are used, when there are withdrawals or deposits to financial accounts and more.

6. Watch your mailbox

Stolen mail is one of the easiest paths to a stolen identity. Have your mail held if you’re out of town. Consider a U.S. Postal Service-approved lockable mailbox. You can also sign up for Informed Delivery through the USPS, which gives you a preview of your mail so you can tell if anything is missing.

7. Shred, shred, shred

Any credit card, bank or investment statements that someone could fish out of your garbage shouldn’t be there in the first place. Shred junk mail, too, especially preapproved offers of credit.

8. Use a digital wallet

If you’re paying online or in a store, use a digital wallet, an app containing secure, digital versions of credit and debit cards. You can use it to shop online or at a compatible checkout terminal. Transactions are tokenized and encrypted, which makes them safer. In addition, contactless transactions have fewer health risks.

9. Protect your mobile devices

Use passwords on your electronic devices. Use a banking app rather than a mobile browser for banking.

10. Check your credit reports regularly

The three major credit reporting bureaus give consumers access to free credit reports weekly, accessible by using AnnualCreditReport.com. Check to be sure that accounts are being reported properly and watch for signs of fraud, like accounts you don't recognize. You

can also sign up for a free credit report and score from NerdWallet to receive alerts when there are changes.

11. Monitor financial and medical statements

Read financial statements. Make sure you recognize every transaction. Know due dates and call to investigate if you do not receive an expected bill. Review “explanation of benefits” statements to make sure you recognize the services provided to guard against health care fraud.

10 ways identity theft happens

Here are some of the ways your personal information can be compromised:

1. Lost wallet

When your wallet is lost or stolen, someone else may gain access to all the information in it.

- Don’t carry your Social Security card or more credit cards than you use regularly, and don’t keep a list of passwords and access codes in your wallet.
- Make photocopies of your credit cards, front and back, and keep them in a secure location so that you can easily call the issuer if a card or your wallet is lost. Some issuers allow you to temporarily “turn off” a lost card; with others, you have to cancel and get a new card issued.

2. Mailbox theft

Someone simply takes your mail or forwards your mail to a different address, so that you suddenly stop getting most mail.

- Sign up for USPS Informed Delivery. You’ll get an email with images of the items that should be delivered to you so you’ll know if things are missing.
- Choose a secure mailbox and retrieve mail promptly.

3. Using public Wi-Fi

Hackers may be able to see what you are doing when you use free public Wi-Fi.

- Don’t use public Wi-Fi for shopping, banking or other sensitive transactions.
- If you choose to use public Wi-Fi, use a virtual private network service to create a secure connection.

4. Data breaches

Hackers invade databases holding sensitive information. Almost everyone has been affected by a data breach.

- Assume that your data is already out there and take precautions accordingly.
- Check your credit scores often — unexpected changes can be a clue — and read financial and insurance statements carefully. Monitor your credit reports, especially for new accounts or inquiries resulting from credit applications.

5. SIM card swap

This is when someone takes over your phone number. You may stop getting calls and texts, or you may get a notice that your phone has been activated.

- Set up a PIN or password on your cellular account.
- Consider using an authentication app for accounts with sensitive financial information.

6. Phishing or spoofing

Some fraudsters try to get you to disclose personal data, such as credit card numbers, Social Security numbers and banking information, by sending an official-looking email. Spoofing involves doing much the same thing with caller ID, so that the number appears to be that of a trusted company or government agency.

- Do not give out personal data in response to an email or call.
- Find contact information from a trusted source, such as your bank website, and use it to verify whether the call or email is legitimate.

7. Skimming

Skimming is getting credit card information, often from a small device, when a credit card is used at a brick-and-mortar location such as a gas pump or ATM.

- Use cards with chips, which have added protections.
- Pay inside at the gas station if you can, because skimming devices are more likely to be placed at unmonitored payment sites.
- Detect fraudulent activity early by setting email or text alerts that let you know when your credit cards are used. If a card is used without your authorization, call the issuer immediately.

8. Phone scams

You may be told you have won something or even that you are in danger of being arrested. The caller claims to need personal, banking or credit information to verify your identity or to know where to send you money.

- Don’t give personal information out over the phone.
- Be aware of common phone scams. The IRS, for example, does not initiate contact with taxpayers by phone (or email or social media) to request personal or financial information, nor does it call with threats of arrest or lawsuits.

9. Looking over your shoulder

Fraudsters can learn a password just by watching your fingers as you key it in. The information on your credit card can be photographed with a smartphone while you shop online in a public place. A business might leave sensitive information where people can see it.

- Be aware of your surroundings.
- Don’t leave cards where they can be seen.
- Cover your hand when you key in passwords or codes.

10. Malware

Opening an email attachment or visiting an infected website can install malicious software on your computer, such as a keylogger. That does what it sounds like — logs every keystroke, giving criminals access to passwords, account numbers and more.

- Be cautious about clicking on attachments or links in emails and about the websites you visit.
- Use a password manager, which lets you avoid keying in login credentials.

How to report identity theft

The FTC's IdentityTheft.gov is a one-stop shop for information and reporting identity theft. Start with that site and follow its recommended steps to make a recovery plan. You may also need to contact your police department, the Postal Service and the credit bureaus. The IRS has a phone line for identity theft, at 800-908-4490, and a taxpayer guide to identity theft on its website.

The FTC takes scam and identity theft reports over the phone or online in multiple languages including Spanish, Mandarin, Tagalog, Vietnamese, French, Arabic, Korean, Russian, Portuguese and Polish. It also offers consumer education in a variety of languages.

You can also go directly to your credit card issuer if your credit card was lost, stolen or used without your knowledge. If it appears someone else used your health benefit, contact your health insurer and consider contacting any involved providers to make sure someone else's health history is not mixed with yours.

What happens when you report identity theft?

Reporting identity theft starts an investigation and the process of restoring your good name. The exact steps will depend on the type of identity theft.

Credit card issuers generally replace the cards with new ones with a different number, and you are back in business. Taxpayer identity theft or theft of benefits typically are resolved more slowly.

No matter which type of identity theft you experience, keep extensive notes about phone conversations and retain related emails.

What is the best identity theft protection service?

Identity theft protection services let you know that your identifying information has been used, or that it is at risk because it was exposed in a data breach. If you are a victim of identity theft, they may also guide you — and reimburse you for costs — through the process of cleaning up the mess and restoring your identity.

If you're already doing all you can do to protect your identity or feel you don't have time to do it, you may want to consider an identity theft protection service. Protections vary, and most offer additional ways to protect your privacy and other services. The best choice among the paid services is one that fits your budget and offers you the coverage you care about.

Before you pay for one, though, check to be sure you don't have an identity theft benefit or discount you're not using.