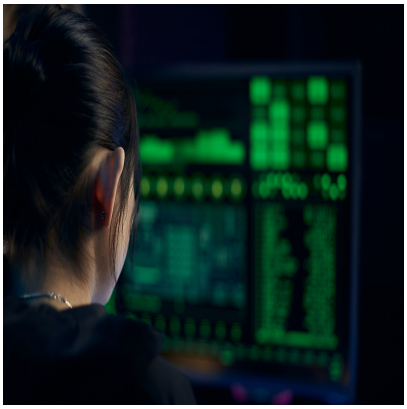
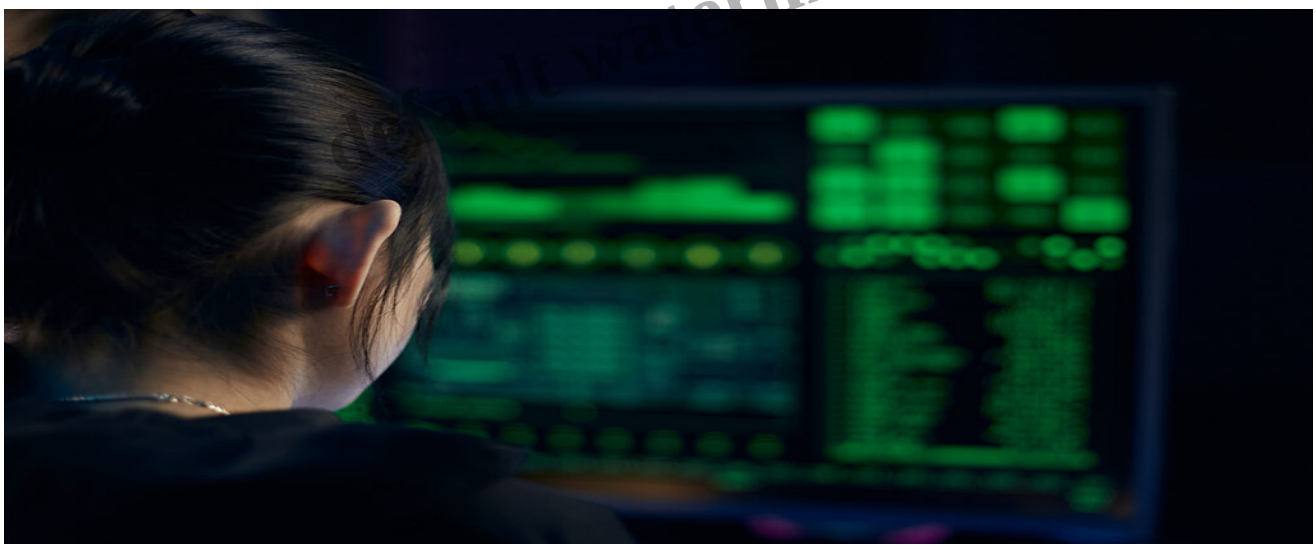


Learn What Identity Theft Is & How to Prevent It with Warning Signs and Tips

Description

ID theft occurs when someone fraudulently acts as you in order to obtain money. Learn about the warning signals and how to avoid them.



Identity theft occurs when someone impersonates you using your personal information — your name, Social Security number, birth date, and so on — and then steals from you.

It’s a rising problem in the United States, and pandemic relief exacerbated it as identity thieves targeted relief cheques and jobless assistance. Theft of benefits increased by a startling 2,920 percent in 2020 compared to 2019. In total, the Federal Trade Commission received 1.4 million consumer complaints of identity theft in 2020, a 113 percent increase from the previous year.

Here’s what you need to know to lower your chances of being a target, recognize warning signs, and act quickly to minimize harm.

What exactly is identity theft?

Identity theft occurs when someone utilizes your personal data to impersonate you or steal from you. Identity thieves may deplete your bank and investment accounts, create new credit lines, obtain utility service, steal your tax refund, use your insurance information to obtain medical treatment, or provide authorities with your name and address when they are arrested.

Because of the frequency of data breaches, your information may already be at risk. In this new world, it's prudent to take precautions to keep criminal actors from stealing your personal information and harming your financial situation.

In this new world, it's prudent to take precautions to keep criminal actors from utilizing your personal information and damaging your financial life.

7 types of identity theft and the warning signs

Once a criminal has your information, these are some common ways it might be used:

1. Credit identity theft

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

Warning indicators include an unusual change in your credit scores or the appearance of an account on your credit reports that you do not recognize. You may receive debt collection notices or a court judgment against you. The best way to avoid it is to freeze your credit.

2. Identity theft in children

Criminals take a child's identity and apply for credit under the child's name. It is often not detected until the victim applies for student loans or other forms of credit.

Investigate if your youngster is receiving credit card offers or phone calls regarding late payments or debt collecting. You can place a credit freeze on your child's account to avoid this.

3. Theft of a false identity

Synthetic identity theft occurs when criminals employ a patchwork of identification details to create a synthetic consumer, combining a Social Security number — frequently one of a small child or one made up — that is not yet in the credit bureaus' database with a name and address. They then seek loans and credit cards, often making payments for years as their credit limits increase. Then there's a "bust out," in which the crooks' cards are maxed out, and they vanish.

If you try to freeze your child's credit and discover that their Social Security number is already in use, this is a red flag. Often, it is not detected until the youngster applies for student loans. It is not always prevented since thieves can make up and use a Social Security number before it is assigned.

4. Taxpayer identity theft

Fraudsters may use your Social Security number to make a tax return and take your tax refund or credit.

You may be unable to e-file because someone else has already filed under that Social Security number, you may receive an IRS notice or letter referencing some activity you were unaware of, or IRS records may suggest you worked for an employer you did not work for. Filing early can help you beat crooks to the punch, and some jurisdictions offer six-digit identity protection PINs (after rigorous verification) for added security.

5. Medical identity theft

Using someone else's identity to obtain health care services is considered medical identity theft. It's especially problematic since it can lead to medical histories getting mixed up, giving doctors and hospitals incorrect information as they make healthcare decisions.

Warning signs: Claims or payments on your insurance explanation of benefits that you do not recognize may indicate that someone is abusing your healthcare coverage. If you've been a victim, you'll need to notify your insurance company as well as your health care team to ensure that the information in your health care records is genuinely yours.

6. Account takeover

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

An email, letter, or text from your financial institution alludes to an action (such as a password or email change) or transaction you do not recognize.

7. Criminal identity theft

Criminal identity theft happens when someone provides law enforcement with someone else's name and address during an arrest or investigation. This is frequently done with fraudulent identification, such as a forged driver's license.

Warning signs: You may be detained by a police officer for reasons unknown to you, or you may be denied work or a promotion because of anything discovered in a background check.

11 strategies to protect yourself from identity theft

You're unlikely to find a foolproof method of preventing identity theft, and monitoring services only notify you after anything has gone wrong. But there are 11 things you can do to make it far more

difficult for identity thieves.

1. Put your credit on hold

Freezing your credit with all three leading credit agencies — Equifax, Experian, and TransUnion – restricts access to your information, making new credit files impossible to open. It is free to freeze your credit and unfreeze it when you open an account. It gives the best security against an identity thief utilizing your details to open a new account.

2. Keep your Social Security number secure

Your Social Security number is the master key to your personal information. Protect it as much as you can. When you are requested for your phone number, inquire why it is required and how it will be safeguarded. Don't bring your card with you. Store or discard documentation with your Social Security number in a secure location.

3. Be wary about phishing and spoofing

Scammers can make phone calls that appear to be from government agencies or businesses, and emails that appear to be authentic may be attempts to steal your information. Rather than responding to a phone or email, initiate a callback or return an email from a known entity such as the official website. Also, be aware of attachments, as many include spyware.

4. Use solid passwords and include an authentication process

Use a password manager to generate and store complicated, one-of-a-kind passwords for your accounts. Passwords should never be reused. Using authenticator software can help to lower your risk. Don't rely on security questions to keep your tabs private; your mother's maiden name and your pet's name aren't challenging to find. Think carefully about what you post on social media to avoid giving away sensitive information or hints about how you respond to security questions.

5. Utilize alerts

Many financial institutions will notify you via text or email when transactions are made on your accounts. Sign up to get notified when and when your credit cards are used, withdrawals or deposits to financial statements, and more.

6. Watch your mailbox

Stolen mail is one of the quickest ways to a stolen identity. If you're going out of town, have your mail held. Consider a lockable mailbox that the United States Postal Service approves. You can also sign up for Informed Delivery through the USPS, which offers you a preview of your mail so you can see if anything is missing.

7. Shred, shred, shred

Any credit card, bank, or investment statements that someone could find in your garbage should not have been there in the first place. Shred junk mail as well, especially pre-approved credit offers.

8. Make use of a digital wallet

If you're purchasing online or in a store, utilize a digital wallet, an app that contains safe, 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, making them safer. In addition, contactless purchases pose fewer health concerns.

9. Keep your mobile devices safe

Mobile devices can pose a severe threat. According to the Javelin survey, only 48% of us frequently lock our mobile devices. Use passwords on your electronic gadgets. When banking on your mobile device, use a banking app rather than a mobile browser.

10. Check your credit reports frequently.

The three major credit reporting bureaus provide consumers with a free credit report every week until April 20, 2022. Check to ensure that any accounts in forbearance or deferment are correctly reported, and keep an eye out for any indicators of fraud. You can also sign up for a free credit report and score from NerdWallet and receive alerts when there are changes.

11 Maintain a close eye on financial and medical statements

Examine the financial statements. Make sure that you recognize every transaction. Know the due dates and contact to inquire if you do not receive an expected bill. To prevent health care fraud, review "explanation of benefits" statements to ensure you recognize the services offered.

10 ways identity theft happens

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

1. Misplaced wallet

Someone else could obtain access to all of the information in your wallet if it is lost or stolen.

- Don't carry your Social Security card or more credit cards than you need, 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 safe place so you can quickly contact the issuer if a card or your wallet is missing. Some issuers allow you to temporarily "turn off" a lost card; others require you to cancel and request a replacement card.

2. Mailbox robbery

Someone takes your mail or forwards it to a different address, and you suddenly cease receiving most letters.

- Sign up for USPS Informed Delivery. You'll receive an email with photographs of the products that should be sent to you, so you'll know if anything is missing.

- Choose a secure mailbox and retrieve mail as soon as possible.

3. Using public Wi-Fi

When you utilize free public Wi-Fi, hackers may be able to see what you're doing.

- Don't use public Wi-Fi for shopping, banking, or other significant transactions.
- If you opt to utilize public Wi-Fi, use a virtual private network service to build a secure connection.

4. Data breaches

Hackers break into systems containing sensitive information, as seen in the 2017 Equifax credit bureau attack. A data breach has affected almost everyone.

- Assume your data is already out there and take appropriate protection.
- Check your credit scores frequently — sudden changes can be an indicator — and carefully study financial and insurance statements. Keep an eye on your credit reports, especially for new accounts or inquiries stemming from credit applications.

5. SIM card swap

This is when someone takes over your phone number. You may stop receiving calls and texts, or you may receive notification that your phone has been activated.

- Set up a PIN or password for your cellular account.
- Consider employing an authentication app for accounts that include sensitive financial information.

6. Phishing or spoofing

Some fraudsters attempt to convince you to reveal personal information such as credit card details, Social Security numbers, and banking information by sending an official-looking email. Spoofing requires performing the same thing with caller ID. The number looks to be from a reputable corporation or government organization.

- Do not respond to an email or phone call with personal information.
- Find contact information from a reliable source, such as your bank's website, and use it to confirm whether the call or email is genuine.

7. Skimming

Skimming is the theft of credit card information, usually from a tiny device, when a credit card is used at a physical place such as a gas pump or ATM.

- Use cards with chips for extra security.
- Pay inside the petrol station if possible because skimming devices are more likely to be installed at unmonitored payment locations.
- Set up email or SMS notifications to notify you when your credit cards are used to detect fraudulent behavior early. If a card is used without your permission, contact the issuer

immediately.

8. Phone scams

You may be informed that you have won something or that you are at risk of getting jailed. The caller claims to require personal, banking, or credit information to authenticate your identity or know where to pay money to you.

- Don’t hand out personal information over the phone.
- Be wary of typical phone scams. The IRS, for example, does not approach taxpayers by phone (or email or social media) to request personal or financial information, nor does it call with threats of jail or lawsuits.

9. Looking over your shoulder

Fraudsters can learn a password simply by watching your fingers as you type it in. While shopping online in a public setting, the information on your credit card can be photographed using a smartphone. A company may leave sensitive data exposed to the public.

- Be alert of your surroundings.
- Do not leave cards where they can be seen.
- Cover your hand when entering passwords or codes.

10. Malware

Opening an infected email attachment or visiting an infected website can install malicious software on your computer, such as a keylogger. That does exactly what it says: it logs every keystroke, providing hackers access to passwords, account numbers, and other sensitive information.

- Use caution while opening attachments or clicking on links in emails and when visiting websites.
- Use a password manager to avoid entering login information.

How to Report Identity Theft

Identitytheft.gov is a one-stop-shop for information and reporting identity theft. Begin with that site, managed by the Federal Trade Commission, and follow the procedures it recommends for creating a recovery plan. You may also need to notify your local police agency, the US Postal Service, and credit bureaus. The IRS offers a phone number for identity theft at 800-908-4490 and a taxpayer guide to identity theft on its website.

You can also contact your credit card company directly if your card was lost, stolen, or used without your knowledge. If it appears that someone else utilized your health benefit, notify your health insurance and consider contacting any associated providers to ensure that someone else’s health history is not combined with yours.

What happens if you report identity theft?

Reporting identity theft initiates an investigation and the process of recovering your good name. The specific methods will vary depending on the sort of identity theft.

Credit card companies usually replace the cards with new ones with a different number, and you're back in business. Taxpayer identity theft or benefit theft is often resolved more slowly.

Keep detailed notes on phone conversations and emails relating to identity theft, regardless of the kind.

What is the best service for preventing identity theft?

Identity theft protection services notify you if your identifying information has been utilized or is in danger due to a data breach. Suppose you are a victim of identity theft. In that case, they may also advise you — and reimburse you for fees incurred — through the process of clearing up the mess and recovering your identity.

Suppose you've done everything you can to safeguard your identity or don't have time to do so. In that case, you might want to think about using an identity theft protection service. Protections differ but must include additional ways to protect your privacy and other services. The ideal paid service matches your budget and provides the coverage you require.

But, before you pay for one, make sure you don't have an identity theft benefit or discount that you're not taking advantage of. For example, suppose the 2017 Equifax data breach harmed you. In that case, you are entitled to identity restoration services even if you did not register a claim.

Category

1. Lifestyle

Date Created
December 2021
Author
tca-admin