



IDENTITY THEFT

What It Is, How to Prevent It, Warning Signs and Tips

Identity theft occurs when someone impersonates you using your personal information, such as your name, Social Security number, birthdate, etc., usually in order to commit a crime against you.

Main types of identity theft that can impact you

<p>Financial Identity Theft</p> <p>When someone utilizes the information of another person for financial benefit, this is the most widely recognized type of identity theft. For instance, an identity thief might open a new credit card using your Social Security number or bank account information in order to steal money or make purchases.</p>	<p>Social Security Identity Theft</p> <p>Your Social Security Number can be used by identity thieves to apply for credit cards and loans and then use it to avoid paying back any existing accounts. Your number may potentially be used by scammers to obtain insurance, disability payments, and other benefits.</p>	<p>Medical Identity Theft</p> <p>The unauthorized use of a person's health insurance to obtain payment for medical services given to a person who isn't covered by the policy is known as medical identity theft. Sometimes, employees or outside hackers steal the data in order to sell the personal data to make money.</p>	<p>Criminal Identity Theft</p> <p>Criminal identity theft occurs when a person arrested by law enforcement uses someone else's name instead of providing theirs. They might be able to pass this off by creating a fake ID or using a stolen ID, like your driver's license, to show to the police.</p>
---	---	---	--



Types of phishing attacks

<p>Smishing</p> <p>The practice of tricking a user into downloading malicious software or a virus using a bait-and-switch text message (SMS).</p> <p>mobile devices</p> <p>Your phone alerts you via SMS or text message that you have won a gift card. When you click the link to redeem, software that logs all keystrokes is installed.</p>	<p>Email phishing</p> <p>Obtaining personal information from a victim while posing as a reputable business.</p> <p>email, websites, social media, mobile apps</p> <p>You receive a fake security warning from your bank requesting that you enter your username and password.</p>	<p>Spear phishing</p> <p>Spear phishing targets a particular group or kind of person, such as the system administrator for a business.</p> <p>websites, email</p> <p>A group of HR experts receives an Excel document titled "2023 Payment Plan." Then an installed flash object collects system login information when opened.</p>
<p>Vishing</p> <p>Fraudulent phone calls intended to collect sensitive personal data.</p> <p>mobile devices, telephones</p> <p>You receive a call from your "phone company" with a special offer for a cheap contract that needs to be paid for right away with a credit card.</p>	<p>Whaling</p> <p>A whaling attack is directed at high-level executives. Attackers pose as trustworthy entities to steal money or information.</p> <p>email, social media</p> <p>A CFO posts on social media about going on a tournament. One of the co-sponsors sends an email with the subject line "Great Game on Sunday." In the email is a picture that exposes valuable info.</p>	<p>Pharming</p> <p>Pharming directs victims to an attacker-controlled website by executing malicious code on their victim's device.</p> <p>websites, computers</p> <p>When you visit your bank's website as usual, you get a notification of a remote sign-on asking you to enter your PIN to unlock your account because your data has been stolen.</p>
	<p>Search engine phishing</p> <p>Involves hackers creating their own website and getting it indexed on legitimate search engines.</p> <p>websites</p> <p>You search for a job online. A fake job offer is presented, requiring individuals to enter their social security number.</p>	

Ways to prevent identity theft

Use strong passwords

A significant security risk is posed by using the same password for all of your electronic devices and important financial accounts. If you use the same password, a scammer only needs to crack one password to access all of your accounts.

Never use your name or birthday as a password, and change it whenever you think an account may have been compromised.

Bonus Tip: Use a password manager to remember and protect your passwords.

Check your credit reports frequently

Your financial account activity, including last-reported balances, is reflected in your credit reports. So checking your credit report frequently is a good way to find errors.

Bonus Tip: If a regular bill doesn't arrive, call or log in directly to your account to make sure a thief hasn't redirected your mail to another address.

Use a Virtual Private Network

In general, you should avoid using a public Wi-Fi network to log into significant accounts or enter payment information. Even networks with password protection might be risky if the password is readily available, like at your neighborhood coffee shop.

A VPN can establish an encrypted connection between your computer or mobile device and the VPN server if you plan to use public Wi-Fi. This configuration can reduce the likelihood that someone will steal your information, but it won't shield you from all attacks or scams.

Bonus Tip: Remember, if your home network doesn't already have one, to add a password.

Watch out for suspicious emails/websites

Never click on any links that seem suspicious in emails or text messages. Identity thieves use emails and websites that appear to be from your bank, credit card company, mortgage lender, or other financial institution to trick you into entering your account information or other private data in a cyberattack known as phishing.

These emails may even ask you to open an attachment that installs harmful malware on your device.

Safeguard your private documents

If handled improperly, physical documents can pose a security risk. Your Social Security number and information about your bank accounts could be found in these documents, which could be useful to identity thieves. A few strategies can be used to defend yourself.

Mailboxes should never be left unattended because identity thieves frequently target them.



Use two factor authentication

2FA is an additional security measure used to confirm that users attempting to log into an online account are who they claim to be. A user must first enter a username and password. After that, they won't be granted access right away but rather will need to provide more information.

