Identity Theft

IDENTIFYING IDENTITY THEFT

Identity theft is a federal crime. It occurs when someone uses your personal information without your knowledge or permission for financial or other gain.

And it's one of the fastest growing crimes in America. Prime targets include children, college students, military members, veterans and seniors, but can happen to anyone at any time.

Typical identity theft involves a thief stealing your personal information to pose as you in some way. A newer and growing variety is called synthetic identity theft. In synthetic identity theft, your personal information is combined with fake data to create a brand new, bogus identity. A thief may combine your social security number with a different name or other fake credentials. Synthetic identity theft can be harder to detect, which can lead to more damage.

Identity theft can create havoc in your life, so it is very important to know how to protect yourself, detect warning signs and correct problems as they arise if your identity is stolen.

How can identity theft affect me?

Identity theft can damage your finances, credit rating and reputation and complicate many areas of your life. Identity thieves might:

- Drain your bank account.
- Make purchases with your credit cards.
- Open new accounts—bank, cell phone, utility, credit card, etc.—in your name.
- Get identity and government documents issued with your name and their photos.
- Receive medical care under your insurance.
- Take out loans in your name.
- Create a false criminal record for you by using your identifying information when investigated or arrested by the police.

Another growing problem is tax-related identity theft. Using your social security number, an identity thief might:

- File a false tax return and collect a refund.
- Get a job and have earnings reported as your income.

Identity Theft

TRADITIONAL TACTICS

Identity thieves continue to use simple, time-tested methods to steal your identity.

Mail Theft

- Use a locking, security mailbox if possible, or consider renting a PO Box at your local post office.
- Put outgoing mail into a postal mailbox.
- Sign up for the free Informed Delivery service offered by the US Postal Service. It provides digital previews of mail scheduled to arrive soon.

Dumpster Diving or Trash Theft

- Shred unwanted documents containing personal information and all unsolicited credit card or loan offers.
- Invest in a high-quality cross-cut shredder. Thieves can piece together papers shredded into horizontal strips.

Shoulder Surfing

- "Shoulder surfers" observe your actions or eavesdrop on stealing personal information and may use a phone to record you.
- Shield keypads with your hand or body before entering PINs, passwords or card numbers.
- Avoid sharing personal information over the phone in public. If you must, use a low voice and shield your mouth.

Purse or Wallet Snatching

- Carry minimal payment cards.
- Don't carry your social security card, PINs or account passwords and memorize passwords tor keep them safely secured at home.

Information Use to Steal Your Identity

- Full name
- Address (home or other)
- Phone number
- Date and place of birth
- Historical information (mother's maiden name, school names, etc.)
- Social security number
- Driver's license number
- Passport number
- Email address
- Screen or usernames
- Passwords and PINs
- Health plan information
- Geolocation information
- Credit and debit card numbers
- Financial account numbers or information
- Photos, videos or audio files

Identity Theft

AVOIDING SCAMS

Running a scam or fraud is another time-tested method for identity thieves. They may contact you in person, by phone/robocall, mail, online or social media to try to trick you into giving out personal information. Here are some tips to stay safe and avoid scams.

- Be aware of current scams. Watch or read the news. The Federal Trade Commission (FTC), offers information and tips on current scams at **consumer.ftc.gov/scams**. The FBI also offers tips and prevention information about scams at **uspis.gov**.
- Before divulging personal information to anyone, know who you're dealing. Independently verify any information provided. Find the physical address and phone number of who contacted you by yourself. Don't trust email addresses given by unknown people. Search online for a company name and website. Read through the site and read any online reviews of the person or business.
- Never reply to messages asking for personal information, whether the message was sent over the phone or by email, text or through an ad. Do not call phone numbers or click on links containing these messages. You could be a target of phishing.
- Never send money or account information in reply to a notice that you won a prize or lottery.
- Give only to established charities. Avoid pop-up charities that suddenly appear after disasters. Check a charity's trustworthiness with the Better Business Bureau's Wise Giving Alliance site at **give.org**.
- Don't fall for pressure tactics. Never react quickly or impulsively to offers or requests.
- Be wary of "impostor" scams in which a scammer pretends to be someone close to you or an entity you're unlikely to question. Fraudsters pretend to be family members, friends, love interests, government agencies or companies often trying to get personal information.

To report a scam or fraud, contact:

- The local police department and state Attorney General's office
- The Federal Trade Commission **reportfraud.ftc.gov | 1.877.FTC.HELP**
- The Internet Crime Complaint Center **ic3.gov** (online related)
- The US Postal Inspection Service **uspis.gov | 1.877.876.2455** (mail related)

To report other types of fraud, visit the US Department of Justice at **justice.gov/criminal-fraud/report-fraud**

Identity Theft

GUARDING YOUR CARDS

Credit/debit card fraud is a form of identity theft. It occurs when a criminal deceitfully gains access to and uses another person's payment card account. If this happens to you, fraudsters may not stop at racking up charges on your card, both online and in stores. They can cause many other problems, including accessing and changing your personal information.

You can reduce your exposure to card fraud and theft by following basic card account maintenance and safety practices.

- Safely store cards when they are not in use.
- Always memorize your card PINs. Never write them down on cards or share them with others. Change them frequently.
- Make a list of your card account numbers, expiration dates and customer service phone numbers. Keep the list in a secure place that you can access quickly if your cards are lost or stolen.
- Go paperless with bills and statements.
- Check your card activity and bank accounts regularly. Look for unfamiliar charges.
- Don't allow websites to remember your card numbers.
- Use a credit monitoring service. Paid services have more robust monitoring. Free services, such as **creditkarma.com**, let you look up your credit score and tell you if a new account has been created or closed.
- Report and investigate any questionable charges to your card immediately. A thief may first charge a small amount to "test out" using your card. Unwary consumers often do not notice or care about small amounts, making them prime targets for identity theft and fraud.
- When you receive replacement cards, thoroughly destroy the old ones.
- Ask your credit card companies to stop sending balance-transfer checks. Thieves can steal these from your mailbox or trash and use them to access your credit and identity.
- Don't give your card information over the phone unless you have made the call and you know you're dealing with a trustworthy business.

You can stop receiving unsolicited, prescreened offers of credit or insurance by mail as well as by phone or email at **optoutprescreen.com**. There, you can choose the electronic opt-out option for five years or the permanent opt-out option by mail.

Identity Theft

CARD SKIMMING

Credit and debit card skimming is when potential thieves steal or "skim" your card information. They use it to create an illegal copy of your card (called "cloning") or to charge items to your card over the phone or online. Or they may sell it to others to do the same.

Thieves use skimming devices that are small, easily portable and hard to detect. Certain types are illegally installed on ATMs and sales terminals such those on gas pumps.

Card skimmers fit over original card readers. As you insert your card, the account information stored on it is skimmed by the device. Keypad overlays are placed on top of factory-installed keypads. The circuitry inside the overlay stores your keystrokes, such as those you make when you enter your PIN. Thieves also may install hidden cameras to record your entering your PIN. These devices are more often installed on non bank ATMs.

At an ATM or sales terminal, check to see if the colors and materials used match up. Look for an extra piece of plastic or anything that appears added on, wrong or out of place. These can be signs of skimming devices.

Don't use the machine if anything looks suspicious. It's better to be safe than sorry. And remember, if anything looks funny or doesn't feel right, walk away.

Pay it Safe

Whether you are running errands or just out for fun, be vigilant about payment card safety.

- Observe the person you're paying. Make sure that person isn't holding anything like a portable skimmer and that your card doesn't leave your sight. When you receive your card back, double check that it is indeed yours and was not swapped for another.
- Insist on privacy when entering your PIN.
- Check sales vouchers carefully before signing.
- Never leave a line blank on a receipt. Draw a squiggly line through any blank space to prevent an unwanted amount being added.
- Be sure a transaction is complete before you walk or drive away from an ATM machine.
- Always take card sales receipts or ATM transaction slips. Never leave them near the ATM or sales terminal. Save them to compare against account statements. Shred them when no longer needed.
- When eating at a restaurant, ask to pay your bill up front at the sales terminal instead of giving your card to a server, or pay at the table when available.
- Consider using Apple Pay or Google Pay with your mobile device. Cashiers can't see your card number, and the process is secure.
- Consider using RFID-blocking card carriers and protectors. Although rare, skimming devices can scan, read and capture information from payment card embedded with RFID tags just by being near them.

Identity Theft

TRAVEL SAFE

Travel can be great, but it can also make you extra vulnerable to identity theft. Here are some things you can do to lower your risk.

Reduce What You Carry

Before you leave, clean out your purse and/or wallet. Remove all unnecessary cards or items. Carry nothing with your social security number on it. Make note of which cards and documents you decide to carry in case of loss or theft.

Be On Alert in Tourist Areas

These are favorite payment card skimming spots as well as popular with purse snatchers.

Avoid Using Public or Shared Computers

They could have information-stealing software in place. If you must use one, avoid entering any personal information or logging onto online accounts.

Avoid Taking Your Checkbook

Your checks show your name, address, bank name, checking account number and checking account routing number—a whole "kit" thieves can use to take over your account. They also can forge checks to withdraw money. If you opt not to use cash or payment cards, use traveler's checks.

Verify Callers to Your Hotel Room

A common scam involves a call to your hotel room from the "desk clerk". This person tells you about a problem that requires you to provide a credit card number over the phone. If this happens, hang up and call or visit the front desk to check.

Downsize Delivery Dangers

Thieves slip made-up flyers for fake food delivery services under hotel room doors, hoping you will call and order using your credit card. Check the reliability of all fliers with the front desk.

Be Careful When Using Wi-Fi

Airports, hotels and other public places offer Wi-Fi for Internet access. A secure wireless network encrypts all the information you send using that network. However, Wi-Fi hotspots are often not secure. This measures information you send though some websites or mobile apps can be accessed by other network users. If you choose to use public Wi-Fi, be very cautious.

- Make sure it's an authenticated Wi-Fi network. Always manually select network connections and know the exact name of the establishment's network. Scammers may set up "free" computer-to-computer networks with look-alike names to fool you.
- Never log in or send personal information to unencrypted website and be aware that for security, the site should be fully encrypted.
- Always log off an account as soon as you have finished using it.
- Consider a VPN (virtual private network) service to protect your information when using public Wi-Fi.

Identity Theft

CYBER THREATS

While computers and the Internet offer huge benefits, they also offer cyber criminals opportunities to steal personal information. Cyber crooks have shown they can keep up with the fast-paced growth of technology. They constantly develop new tools and methods to trick and exploit people though computer and Internet use. The more aware you are of cyber threats, the more prepared you are to avoid them.

"Malware" is a broad term for the many forms of malicious software designed to disrupt, harm or hijack a computer system or data. It includes viruses and spyware. Secretly installed without your knowledge or consent, malware programs can damage your privacy and the security of your computer or mobile device. They can capture your personal information in a variety of ways and secretly send it to identity thieves.

Computers and mobile devices are commonly infected with malware through email attachments, downloads and the links within emails or pop-up windows.

Carefully read all disclosures, including the privacy statement and licensing agreement, before downloading and installing software. Malware may be bundled in with it. Look for wording about personal information collection, Internet activity monitoring or additional programs.

Warning Signs of Malware

- Slow or sluggish performance
- Computer crashes
- Repeated error messages
- Being automatically sent to websites you didn't mean to visit
- An unintended reset to a new Internet home page that can't be undone
- Getting bombarded with pop-up ads and/or ads popping up when a browser is not open
- Finding a new toolbar added to your browser
- Seeing new icons on your desktop
- Your online search results page shows only ads
- Emails sent from your account that you didn't write
- Decreased battery life, interrupted or dropped calls and crashing apps on mobile devices are also warning signs of a malware infection

Malware can be hard to remove. If you suspect it immediately stop all online activities that require you to enter any kind of personal information, update and then run your security software and seek reliable tech support if possible.

Identity Theft

CYBER THREATS (cont.)

Catfishing

When a person creates a fake identity on social media, usually targeting a specific victim for abuse, deception or fraud. Catfishing is often used for romance scams on dating website.

Phishing

When cyber thieves send you emails that try to lure you into providing or confirming personal information. The emails look like they're from legitimate organizations, often ones you know. These ordinarily used threats, warnings or enticements to create a sense of urgency. You're usually asked to click on a link. If you do, it can lead to a spoof website. The site looks real enough to trick you into entering personal information. Signs of phishing emails could include:

- Request (usually urgent) for you to make contact through a provided link
- Spelling and grammar mistakes
- Generic greetings, like "Dear User"
- Unsolicited attachments

Smishing and Vishing

Very similar to phishing, this is when criminals use automated dialing systems to call or text you with messages intended to trick you into sharing personal information. The message will direct you to a phone number or website that asks you for the information.

Clicking on links, opening attachments or going to web addresses provided through phishing, smishing and vishing frequently cause identity-stealing malware downloads.

Avoid Phishing, Smishing and Vishing

- Never click on links from unknown senders. Be cautious about clicking emails and text message links even from known senders.
- Don't trust contact information provided in emails, text messages or pop-ups. Verify it on your own.
- Don't respond to text or automated voice messages on your mobile phone if they're from an unknown or blocked called.
- Know that most legitimate companies and organizations won't request personal information via email.
- Be cautious about downloading email attachments. Ensure you know and trust the sender.

Identity Theft

BE CYBER SECURE

Always make sure you have up-to-date and active security software to protect yourself.

Firewall Protection

A firewall is basically a software program or a piece of hardware that helps to screen out malware and hackers that try to reach you through the Internet while you are on it.

Anti-Virus and other Anti-Malware Programs

Don't assume an anti-virus program offers protection against all kinds of malware. Viruses are one type of malware. Other types, including the information-stealing malware known as spyware, may not be covered by an anti-virus program. Investigate security software programs and make sure yours is comprehensive.

In addition, here are some additional ways to keep you cyber secure.

1. Always update. Keeping your operating systems, security software programs and browsers current can help secure your identity. Updates provide new patches for any security weaknesses.
2. Evaluate your browser's privacy settings, plus think about limiting or disabling cookies—those tiny bits of data used by web servers to identify users. Some cookies are useful, but others can be used maliciously and collect information about you.
3. Explore security options for all devices that connect to the Internet, including gaming systems.
4. Make sure mobile devices aren't set to automatically connect to nearby Wi-Fi, as this can expose you to unsecured network.
5. When not in use, disable mobile device features that connect you to other devices.
6. Set mobile phones, tablets and laptops to lock automatically after five minutes or less of non-use.
7. Back up your data regularly.
8. Before disposing of a computer, mobile device or any Internet-connected item, completely and permanently remove all personal information from it.
9. If you use an at-home wireless network, take steps to secure it. Otherwise, unauthorized users may be able to access your personal information, see what you're transmitting and download malware.
    - Make sure your wireless router's encryption feature is turned on.
    - If your wireless router comes with a built-in firewall feature (which is typical), turn that on.
    - Change the default name the manufacturer gave the router to one only you would know.
    - Routers also come with a default password. Change it to one that's hard to crack.
    - Many router manufacturers release security updates. Regularly check for new firmware updates.

Identity Theft

BE CYBER SECURE (cont.)

- Create strong passwords that are at least 10-12 characters long and include a combination of capital and lowercase letters, digits and special characters. Don't make them predictable. Change them frequently.
- Consider using a password manager to create complex passwords without needing to remember them.
- Don't use the same password for multiple accounts.
- Don't open emails from unknown senders.
- Never email financial information or your social security number.
- Download software or email attachments only from sources you know are trustworthy.
- Read all disclosure information before downloading software, including apps.
- Always type authenticated web addresses directly into your browser bar instead of clicking links.
- Limit what you share on social media. Consider increasing your privacy settings.
- Don't stay signed into accounts. When you are finished, log off and close your browser.
- Close all pop-up windows by clicking on the "x" in the title bar. Consider using a pop-up blocker.
- Don't put unknown flash drives into your computer. Use two-factor authentication for online accounts when available. This is when you provide two different ways to verify yourself, such as a password and a phone number, to better protect you.

Identity Theft

SHOPPING SAFE ONLINE

Before you create an online account, shop or enter any personal information on a website, check for signs that the organization and the site is secure and trustworthy.

Look for Security Indicators

The "https" at the beginning of the web address indicates the page uses a secure form of encryption to protect the information you enter. Most browsers use other security indicators—a symbol, such as a padlock and/or a color change. Learn how your browser reports website security levels but remember, indicators are not foolproof.

Learn About Who You Are Doing Business With

Research businesses on the Better Business Bureau's website, **bbb.org** or through an online search. Read the reviews. Confirm the business or seller's physical address and phone number. Legitimate entities provide this so you can contact them with problems.

Read the Privacy Policy

Understand what personal information the site collects, how it's used and if it's shared. Learn what security measures are used to protect your information.

Do Your Research

Read through return, refund or shipping policies, terms of use and other information provided about the establishment, its site and how it conducts online businesses.

Guard Your Cards

Shop online with a credit card rather than a debit card, which provides direct access to the money in your bank account.

Identity Theft

WORKPLACE IDENTITY THEFT

No matter how comfortable or familiar you may feel on the job, you need to protect against workplace-related identity theft risks. You also have a responsibility to protect the personal or sensitive information of your colleagues and employers. If you deal with the personal information of customers or clients, your responsibility is even greater.

For everyone's sake, including your own, make sure you understand and follow all organization security and privacy policies. Practice good online and offline identity protection habits.

- Lock up your purse or wallet when it's not with you. Too often, payment cards, checks and other identity-related items are stolen at the workplace.
- Also lock up personal and work-issued mobile devices, ID badges and workplace access cards with not in use.
- Don't put your personal information at risk in the case of a workplace security breach. Never reuse personal passwords for work, log into personal accounts from work or store personal data or material on work computers or devices.
- Keep all work passwords and usernames confidential. Don't write them down and store then in your work area.
- Securely store anything with your or others' personal information at the end of your workday.
- Verify the identity of anyone who claims to work for or with your workplace and asks you to share personal or sensitive information in person, online, over the phone or by mail.
- Be aware of who is around you when you input, share or access sensitive information. Shield screens, keyboards or keypads when necessary. If speaking, take eavesdropping precautions.
- Thoroughly shred unwanted documents containing others' personal information.
- Log off and close all screens when you step away from your computer.
- Be extra vigilant about personal information safety when temporary workers, service professionals, delivery people and other visitors are present.
- Watch out for phishing targeted to employees at your workplace.
- Don't assume work computers, software and Internet security systems will prevent you from accidentally introducing malware. You share in the responsibility of keeping your organization's system safe.
- Immediately report any signs of suspicions of malware or security breaches according to your employer's procedures.

Identity Theft

SIGNS OF IDENTITY THEFT

Many people don't know they've become victims of identity theft until they're contacted by a financial institution. Early detection can help limit the damage done by an identity thief. Here are indicators that you may be a victim of identity theft.

- You notice errors or unfamiliar transactions on your bank and/or credit card accounts.
- Your credit report includes unfamiliar accounts or charges.
- Your credit report contains inquiries made by businesses in response to applications for credit, loans or services you didn't initiate.
- You receive collection notices or calls about a debt that isn't yours.
- You have a good credit rating but are denied credit in response to an application.
- Your checks are refused by merchants.
- Bills, statements and other expected mail or email doesn't arrive.
- You get bills for accounts you didn't open or medical services you didn't receive.
- Your health insurance responds to your legitimate medical claim with a notice that your benefits limit was reached.
- Your medical records report a condition you don't have.
- You are notified by the IRS that you have income from an employer unknown to you or that more than one tax return was filed with your social security number.
- You re notified of a data breach at a company that involves your information.

Data Breach

A data breach is any instance in which secure information has been released or stolen intentionally or unintentionally. The organization that exposed or lost your information will notify you and should explain your rights and options. Your state may provide additional rights.

The steps you should take depend on the type of information that was lost or stolen.

- Monitor all bank and other accounts for suspicious activity.
- Change all passwords, PINs or usernames associated with compromised accounts.
- Order a copy of your credit report.
- Place a fraud alert and/or a credit freeze on your credit file.

For more on how to respond to a data breach, visit **identitytheft.gov**.

Identity Theft

IDENTITY THEFT VICTIM: NEXT STEPS

If you become a victim of identity theft, act quickly to help limit the damage.

1. Call any business where you know fraud took place. Ask to speak to the fraud department. Say your identity was stolen. Ask for your account(s) to be closed or frozen so an identity theft can't add new charges.
2. Place an initial fraud alert on your files. Contact one of the three major US credit reporting companies to report yourself as a victim of identity theft and to place the initial fraud alert. That one must tell the other two. Ask the credit reporting company you contact for confirmation that this will be done.
3. A fraud alert on your credit report lets lenders and creditors know that they should take steps to verify your identity before they issue you credit. This may help prevent identity thieves from opening new accounts in your name. An initial fraud alert is good for 90 days and may be renewed. You may later choose to place an extended fraud alert. You might also choose at this time to place a credit freeze.
4. Order a credit report. By law, you are entitled to a fee copy of your credit report once a year from all three companies. You must contract each individually to order a report. You may wish to order one now and the other two at later times to track new activity or corrections. Immediately review your credit report and note any unfamiliar transactions or accounts. Give this information to authorities such as the FTC and the police.
5. File a complaint about the theft with the FTC. You can do so online at **reportfraud.ftc.gov** or by phone at 1.877.438.4338. Include as much information as possible and follow instructions carefully and make sure to save and print out your completed complaint. Once it's printed out, it becomes an Identity Theft Affidavit. The affidavit helps you create an Identity Theft Report.
6. File a police report. Go to your local police station (or the police station where the theft occurred). Say you are a victim of identity theft and wish to file a police report. Bring along the following:
    - A copy of your Identity Theft Affidavit
    - Any other proof of identity theft
    - Proof of your address
    - Government-issued photo ID

You must have a completed Identity Theft Report to prove to businesses that you are an identity theft victim and to exercise all of your rights.

Identity Theft

IDENTITY THEFT VICTIM: NEXT STEPS (cont.)

Be Organized and Attentive

As you respond to identity theft, set up a system that helps you track information and deadlines.

- Log every phone call. Write down the date and time, phone number and any other contact information. Also record the name, department and title of the person you spoke with, as well as a summary of the information discussed.
- Confirm discussions in writing with follow-up letters or emails.
- Set up a filing system especially for this issue.
- Never send original documents. Keep them security filed. Send only copies to others.
- Send all letters, documents copies or other materials by certified mail with a return receipt requested. Log who you sent that and when.
- Make and file copies of all the correspondence or completed forms you send. File all correspondence or documents you receive.

Note important dates and deadlines in your calendar. Always learn how long you have to supply information or to have other supply it to you. Once you have taken care of all immediate actions, there are a few more things you can do to continue to limit damage or recover from it. What you do next, including whom you contact, will depend on what personal information was stolen and how far-reaching the theft's effects.

Visit **identitytheft.gov** for specific information, sample letters to send and contact links for various situations.

As you learn of any issues through your credit report or other avenues, respond quickly.

Identity Theft

IDENTITY THEFT VICTIM: ADDITIONAL STEPS TO CONSIDER

Close Fraudulent Accounts

- Call the fraud department of each business and ask for the account to be closed.
- As required, send each business a copy of your Identity Theft Report and/or any completed dispute form it requests along with a letter.
- Ask for a letter that confirms the account was fraudulent, that you are not liable for it and that it was removed from your credit report

Get Proof of Fraudulent Activity

- Ask businesses for copies of documents the identity theft used to open a new account or make a purchase in your name.
- Don't take no for an answer. Speak with a supervisor if necessary.

Get Rid of Fraudulent Charges

- Call the fraud departments of every bank or business to report all wrongful transactions.
- As required, send them copies of your Identity Theft Report and/or any completed dispute from along with a letter.
- Request letters from them that confirm their removal of fraudulent charges.

Correct Credit Report Errors

- Send a letter to the three credit reporting companies requesting all fraudulent information be blocked (removed).
- Enclose a copy of your Identity Theft Report, proof of your identity and copies of documents that show the errors your letter is reporting.

Consider an Extended Fraud Alert

- An extended fraud alert lasts for seven years. Unlike any initial fraud alert, which says creditors should contact you before extending credit in your name, an extended fraud alert required they do so using the contact information you provide when you place the extended alert. You also before entitled to two free copies of your credit report each year.
- If you choose to place one, send a letter of request and a copy of your Identity Theft Report to each of the three credit reporting companies.

Freezing Credit

Also known as a security freeze, this is designed to restrict access to your credit report unless you temporarily lift or permanently remove the freeze. A credit freeze makes it less likely that an identity thief can open a new account in your name. Be aware that a credit freeze can cause delays or other issues when you submit requests or applications that involved your credit report. Ask about such issues and weigh any concerns against your need for identity security.

Identity Theft

RESOURCES

Credit Reporting Agencies

- Equifax | Equifax.com
- Experian | Experian.com
- Transunion | TransUnion.com

Better Business Bureau
bbb.org

The Federal Trade Commission (FTC)
ftc.gov | identitytheft.gov

Internal Revenue Service
irs.gov/identity-theft-central

Federal Bureau of Investigation's Internal Crime Complaint Center
ic3.gov

National Cyber Security Alliance
StaySafeOnline.org

US Department of Homeland Security
dhs.gov | cisa.gov

REV 06.2024 Content sourced from Identity Theft: Protect Yourself, Know What To Do Handbook, Positive Promotions®. Resources subject to change.

Identity Theft

ARE YOU AT RISK?

Mark **T** for true and **F** for false to see how well you protect your personal information from identity thieves.

1. My mailbox has a locking device.
2. I put all outgoing mail into a postal mailbox.
3. I shred all unwanted documents.
4. I use a good-quality crosscut shredder.
5. I carry only the payment cards I need and will be using each day.
6. I know exactly what identity-containing cards, documents and other items are in my purse or wallet at all times.
7. I memorize all my PINs.
8. I shield keypads when entering passwords or card numbers.
9. I change my PINs and passwords often.
10. My passwords are all 10-12 characters in length and a good mix of capital and lowercase letters, digits and special characters.
11. I use a password manager.
12. I carry my social security card only when absolutely necessary.
13. I am very cautious about sharing my social security number and ask why it's needed and how it will be kept safe before I give it out.
14. I don't share personal information with unknown callers.
15. I donate to established charities only.
16. I use a credit monitoring service.
17. I use a VPN when on public Wi-Fi.
18. I never click on links in pop-up windows.
19. I don't click on links in emails or text messages from unknown senders and only do so cautiously from known senders.
20. Before using ATMs and sales terminals, I check for signs of skimming devices.
21. I always take receipts, safely store then and shred them when no longer needed.
22. I don't autosave login information.
23. I stay alert to risks when traveling.
24. My computer and devices have comprehensive security programs.
25. I stay on top of updating operating systems and software.
26. I independently verify web addresses, then enter them directly into my browser's address bar instead of using email links.
27. I download software, apps and email attachments only from reliable sources.
28. I read all disclosure information before downloading software.
29. I limit what I share on social media sites.
30. I don't trust anyone online and know people may not be who they say they are.
31. I secure my at-home wireless network.
32. I use two-factor authentication on online accounts.
33. I keep all computer and Internet-related security and privacy setting at strong, identity-protection levels.
34. I know about and utilize security options for all my Internet-connecting devices.
35. I make sure my mobile devices don't automatically connect to nearby Wi-Fi.
36. I always log off an account and close my browser when finished with an online transaction.
37. I check for signs that a website and its business are secure and trustworthy before entering personal information.
38. I am careful about securely storing personal items I bring to my workplace.
39. I don't store personal information or access personal accounts on work computers or devices.

If all or most of these statements are true, congratulations! You're doing a good job at preventing identity theft. If any were not, consider how you may be putting yourself at higher risk for identity theft.