How To Protect Against Identity Theft

► No one is exempt from becoming a victim of identity theft or fraud. Every two seconds, a person's identity is stolen, and one in fifteen people become victims of identity theft. Learn ways to protect yourself.

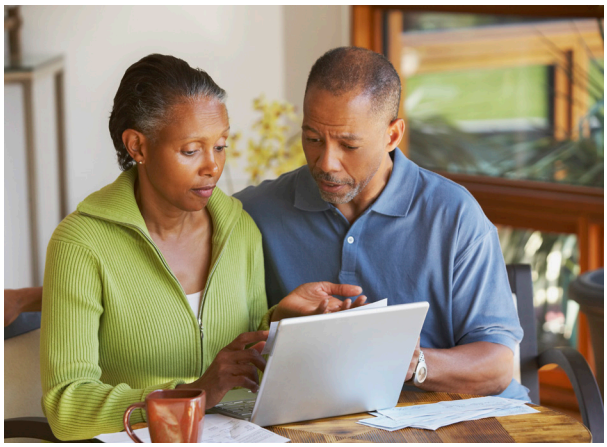
Identity theft and *identity fraud* are terms used interchangeably and refer to all types of crimes. These crimes include an individual illegally obtaining and using another person's personal information that involves fraud or trickery for economic gain. In other words, the identity thief steals and uses another person's personal information without his or her permission. According to the Federal Trade Commission Consumer Sentinel Network, in 2020 Alabama ranked twenty-first in the highest number (17,376) of identity theft cases reported in the United States.

A person's fingerprint is unique to an individual and cannot be given to someone else for their use. However, your personal data, such as your name, Social Security number, bank account or credit card numbers, birthdate, driver's license or other I.D.s, mother's maiden name, and passport, can be used to commit identity theft and fraud. All these items can be an asset to the identity thief.

Your personal financial information is always at risk whether you are using a debit or credit card online, the phone, in person, at a gas station, or in other stores. If your identity is stolen, thieves can personally profit at your expense. They can run up a vast number of debts and commit crimes while using the victims' names. In many cases, a victim's losses may include not only out-of-pocket financial losses but also substantial additional financial costs. These costs are associated with restoring one's reputation in the community and correcting inaccurate information for which the criminal is responsible.

Identity thieves do not discriminate based on race, social-economic background, culture, age, or sex. Everyone must take steps to protect themselves from identity theft. This document includes the following:

- How can your identity be stolen?
- Methods used by criminals to steal your identity



- Types of identity theft
- Warning signs of identity theft
- How to protect your information
- How to report an incident if you are a victim of identity theft

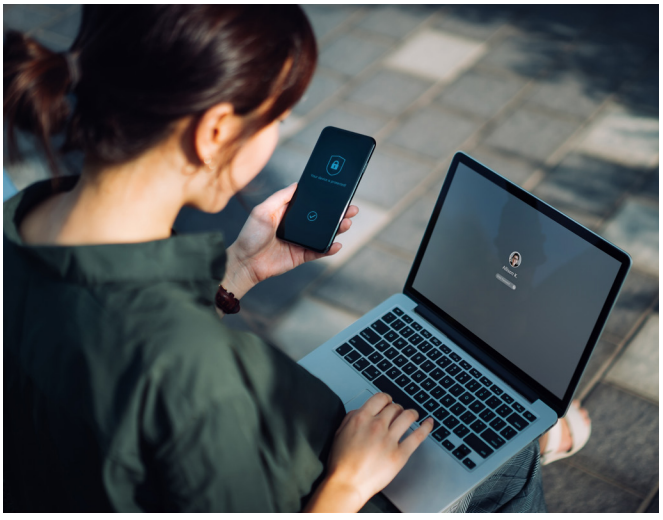
How Can Your Identity Be Stolen?

When an identity thief has enough information about an individual, the thief can take over that person's identity and conduct numerous crimes. These crimes could be anything from making fraudulent withdrawals from bank accounts, filing false applications to obtain loans and credit cards, fraudulently using credit and debit cards to receiving other goods and privileges. As a result, the criminal can use another person's information to obtain goods or services that might otherwise be denied he or she might be denied. Most criminals hide their fraudulently opened accounts by ensuring that bank statements showing the unauthorized withdrawals are sent to an address other than the victim's address. This action delays the awareness of what is happening until the criminal has already inflicted substantial damage on the victim's credit, assets, and reputation.

Methods Used by Criminals to Steal Your Identity

Your identity can be stolen in several common ways. In some cases, identity thieves are known to their victims. For example, your identity can be stolen by family members, friends, or neighbors in addition to strangers who use different methods. Below are a few of the many methods used to steal a person's identity. Be careful to protect your identity.

- **Phishing**. Identity thieves send out phishing emails to trick people into giving out personal information. These emails appear to come from a trusted or known company, such as work, a bank, or an online retailer. Avoid clicking on unknown email links. They could be sent by impersonators.
- **Smishing.** Phishing by text messages is smishing. The scammer sends compelling text messages in an attempt to obtain personal information for profit or economic gains. It is best to delete unknown text messages. Never open a text message link provided by strangers. It could be a hacker trying to access your device to steal information.
- **Vishing.** Phishing by phone calls is also known as voice phishing or vishing. A caller may tell a victim that he or she has won a prize or will be arrested if taxes are not paid. The victim is often provoked into giving out personal information. Whenever someone is asking for personal information, do not be quick to release this information. Ask what they need it for, how are they going to use it, and how will they protect your personal information.
- **Spear phishing.** Any time specific individuals or groups within an organization are targeted, this is called spear phishing. For example, an identity thief can send an online job advertisement to a youth group organization asking members to click on a link to apply. When they click the link and enter personal information, the thief steals the data. Sometimes the thief can lock the computer to prevent the victim from having access. Avoid responding to job opportunities sent by an unknown organization or individual. If you work for a company, always report suspicious emails. If you are in doubt, go with your first instinct. Do not click on a link provided by an unknown sender.
- **Pharming.** The practice of pharming sends victims to what appear to be legitimate and secure websites. But be careful. "Https" does not always indicate a secure site. Criminals have created fake websites known as "honey spots." These websites may look like authentic, trustworthy sites with a familiar logo and similar URL to make people more willing to share personal information. If you fall for this scam, any purchases made on the fraudulent site may never arrive. Also, the thief may plant malware to infect the victim's device and harvest financial or other personal information.
- **Skimming.** Skimming occurs when thieves steal your credit or debit card information when you swipe to make a purchase. In some cases, the thief can use a card reader to capture data while the card is in your purse or wallet. Some may place a recording device at an ATM or a gas pump machine. Check these areas when inserting your credit or debit card to make sure there are no attachments. It is best to use your credit card rather than your debit card when paying at a gas pump. If a thief steals your information, the credit card company can reimburse your money quicker than a bank.
- **Social media scamming.** If you use social media platforms such as TikTok, Facebook, Instagram, Snapchat, Twitter, etc., your risk for identity theft increases because thieves use the information collected to register for sites. Social media scamming can occur if someone uses low privacy or no privacy settings, accepts an invitation to connect from unfamiliar people or contacts, downloads free applications for use on your profile, or gives password or other account details to people you know. These are only a few ways your identity can be stolen. To protect yourself, set privacy settings. Never accept an invitation to connect with people you do not know. Avoid using free downloads and don't give out personal information by sharing your password or other account information.



- **Public USB charging stations and Wi-Fi.** Hackers love to be in public places to scam innocent individuals. When traveling, be aware that public Wi-Fi networks make it easier for hackers to collect someone's private information. Scammers can set up juice jacking USB stations in airports or hotels, for example, causing the malware to infect people's devices when connected. Do not use any public USB charging stations or Wi-Fi if you do not have a VPN or some other type of protection on your device.
- **Data breaches.** No company or organization is exempt from a cyber attack or improper disposal of physical documents. In normal circumstances, an individual is notified of a breach that involves the exposure of their personal information. Criminals can use stolen username and password combinations to hack into other accounts.

Types of Identity Theft

You can fall victim to many types of identity theft: tax, financial, employment, medical, child, and many others. Any of these frauds can be used to steal your identity. Following are suggestions for ways that individuals can protect themselves from becoming victims. Detecting identity theft early is the best response to reversing these illegal acts.

Tax Identity. Tax identity theft occurs when someone uses your personal information to file a tax return in your name. Under normal circumstances, individuals discover tax identity theft when they file their tax returns. Visit the Federal Trade Commission's website on identity theft to learn more.

To protect yourself:

- Store social security cards and all tax records in a safe location in the home or a safe deposit box. Avoid leaving important documents that have personal identifying information out in public view.
- Practice disposing of tax records by shredding or ripping them up. If you don't have a shredder, take advantage of local shredding days in your community.
- Avoid responding to any emails or text messages from the Internal Revenue Service (IRS).
- Never give personal information over the phone to someone who says they are from the IRS. The IRS will never send you an email or text message or call your phone. In other words, the IRS always mails notices and other communications to tax filers.

Financial Identity Theft. Out of all the types of thefts, financial fraud is the most common form of identity theft. This occurs when someone uses your information for financial gain. The thief may use your credit or debit card information or write checks in your name.

To protect yourself:

- Read bank and credit card statements each month.
- Use cash when eating out if you can. If not, use a credit card. In most cases, the identity theft victim will only be liable for the first $50 if your financial information is stolen.
- Use a credit card when at the gas pump.
- Discard all financial documents properly by shredding, ripping them up, or burning them.
- Monitor your bank account online daily or a few days per week. This will help you keep an eye on transactions made. If you see something suspicious, contact your bank as soon as possible.

Employment Identity Theft. No one thinks someone can use their employment information. Depending on how desperate a thief may be, someone can use another person's work information to pass an employment background check to land a job.

To protect yourself:

- When being asked for personal information related to your employment, check the email address to see if it is a personal or business email. It may be a scam if it is from a personal email address rather than a company email address.
- Don't be quick to click on email links when you see familiar coworker names. Verify that it is a person you know and not someone impersonating them.
- Avoid giving out your social security, assigned banner, or work identification number.
- Be on guard when random employers request your bank or credit card information to conduct a background check before an interview or job offer is made.
- Ask why they need this information, how will they use it, and how they will protect it, especially if you have not applied for a job with the requesting company?

Medical Identity Theft. Thieves have also been known to steal a person's personal information to receive medical care in their name. Your medical information is just as important as any other sensitive data. There are a few steps you can take if you receive a medical bill for services that were not provided to you.

To protect yourself:

- Practice reviewing your Explanation of Benefits medical statements sent by your insurance company.
- Carefully look over the document for mistakes.
- Verify that medical services provided were services received by you or a family member.
- Report any services identified on the statement that you did not receive. For instance, services to doctor's offices, an emergency room, hospital, or medical testing center.
- Avoid sharing any personal identifying medical information on the phone or in an email. You could be giving it to a scammer.
- If you are in a public medical setting and you are asked to verify your social security number, do not give it out verbally, especially if people are in your presence. Ask for a piece of paper and write your number on it. After it is keyed in by the receptionist, ask for the paper back and properly dispose of it.

Child Identity Theft. Parents must protect their children's identity. Did you know that children are 51 times more likely to be victims of identity theft than adults, according to a study by Carnegie Mellon University's Club? Because of data breaches, this occurs 65 percent of the time. Consumers can't prevent or predict a data breach that affects a company they do business with or work for. A data breach is one of many ways a child's information can be stolen because they are on their parent's insurance plan. However, there are steps you can take to reduce your risks online and better protect yourself and your personal information.

To protect yourself and your child:

- Tell your children never to leave their belongings out in public view.
- Ask questions before giving anyone your child's Social Security number.
- If your child's school wants a Social Security number, ask these questions:
  - Why do you need my child's information?
  - How will you protect my child's information?
  - Can you use a different identifier for my child?
  - Can you use just the last four digits of the Social Security number instead of the entire number?

Warning Signs of Identity Theft

Certain red flags can let you know that someone has stolen your identity:

- You see withdrawals on your bank statements that you didn't make.
- You experience a debit or credit card transaction not going through.
- You have a monthly statement and missing bills from one month to another.
- You have businesses refusing to accept your checks.
- You are receiving letters in the mail about accounts you did not open.
- You are arrested for a crime you did not commit, but your I.D. was found at the crime scene.
- You have debt collectors calling about debts you did not create.
- Your username and passwords no longer work while you are trying to log in to your device.
- You apply for your first driver's license and are told you already have one.
- You are denied applications for credit cards or student loans, and you have never used your credit.
- Your credit report shows accounts, incorrect addresses, or names you have never used.

How to Protect Your Information

- Guard your personal information and do not have a casual attitude about leaving your belongings (purse, wallet, book bag, etc.) unattended. Leave them in a secured place.
- Never carry your Social Security card in a wallet or purse unless you a going to conduct business.
- Frequently examine bank and credit card statements. Look for purchases or charges you did not authorize.

- Properly discard important papers by shredding all documents with financial information on them (Social Security number, bank and credit card statements, and canceled or unused checks). Also, shred preapproved credit card mail offers and other offers that request personal information before discarding them in the trash.
- Never give out financial information such as a credit card or your social security numbers, over the phone unless necessary. Verify and know who you are speaking to on the phone.
- Avoid using public Wi-Fi when out in public and entering financial information to make purchases. Some criminals create “honey spots,” which are fake websites set up to steal your personal information.
- Practice good cybersecurity habits. Create strong passwords on your computer, phone, tablet, and website accounts. To strengthen your password, use upper- and lowercase letters, numbers, and characters. Change your password often, and do not use the same password twice.
- Avoid clicking on unfamiliar email links. If an email seems suspicious, report it to your information technology department if at work or to your email carrier.
- Order your free annual credit reports. Inspect the reports for any unusual activity like loans you did not apply for or credit card queries from companies you did not authorize to check your credit.
- Consider placing a credit lock on your credit report. Any time a criminal attempts to get a credit card or loan in your name, the creditor will not be able to access your credit report. If you need to apply for a loan, you can unlock it until the loan is approved. Then you can lock the credit report again.
- Use an encrypted website that starts with “https” at the beginning of the address to protect your personal information. However, remember that this does not indicate a secure site.
- Install a firewall, anti-spyware, and anti-virus software on your computer for added protection.
- Clean up your financial trash by shredding your junk mail, bank and credit card statements, and other documents that have your identity.
- Pay attention to your surroundings when using ATMs. Protect your PIN by memorizing it and never writing it down.
- Use direct deposit to keep your payroll check from being delivered by mail and possibly being stolen by an identity thief.
- Don’t let people hear you give your credit card, pin, or Social Security number over the telephone.
- Do not share your password to your computer with others, and do not reply to spam emails.
- Don’t give family members, friends, or neighbors your personal information, such as your pin or Social Security number.

How To Report an Incident if You Are a Victim of Identity Theft

If you are a victim of identity theft, follow these simple steps from the Federal Trade Commission:

- Place a fraud alert on your credit reports and review your credit reports at least once per year. Contact the credit reporting agency that is closest to the state where you live. Remember, you only need to contact one of the three nationwide credit bureaus to place the initial one-year fraud alert, extended fraud alert, or active-duty alert (if on military deployment) on all three of your credit reports. Whichever one you choose will report to the other agencies:
  - Equifax: 1 (800) 525-6285; PO Box 740241, Atlanta, GA 30374-0241
  - Experian: 1 (888) EXPERIAN (397-3742); PO Box 9532, Allen, TX 75013

- TransUnion: 1 (800) 680-7289;
  Fraud Victim Assistance Division,
  PO Box 6790, Fullerton, CA 92834-6790

- Visit AnnualCreditReport.com to order a free copy of your credit report once a year. All citizens of the United States are entitled to a free report from all three credit reporting agencies once per year.
- Close and dispute any accounts that you know or believe have been fraudulently opened in your name. Contact one of the nationwide credit reporting agencies and speak with someone in the security or fraud department. Do a follow-up in writing. Avoid sending original receipts and only include copies of supporting documents. Send letters relating to the theft to notify credit card companies and banks in writing. Make sure that you send a certified letter, in addition to requesting a return receipt. Use this information to document what the company received and when. Keep a paper trail by filing your correspondence and enclosures.
- If you open any new accounts, do not forget to change your personal identification numbers (PINs) and passwords. Avoid using easily obtainable information such as your or your child's birth date and last four digits of Social Security numbers, mother's maiden name, your phone number, or a series of consecutive numbers like 1234. Ask the company for forms to dispute unauthorized transactions only if the identity thief has fraudulently opened accounts in your name.
- File a report with your local police or the police in the community where the identity theft took place. Contact your local police department and inform them that you want to file a report about your identity theft. Check to see if you can file the report in person. If not, ask if you can file a report over the telephone or the Internet. If the police are reluctant to accept your report, request to file a miscellaneous incident report, or try another jurisdiction such as your state police. Take with you a copy of the Federal Trade Commission's Identity Theft Complaint form, your cover letter, and any other supporting documents to help the police understand why police reports and identity theft complaint forms are so vital to victims.
- File a complaint with the Federal Trade Commission (FTC) by using the online complaint form or call the FTC's Identity Theft Hotline toll-free at 1 (877) ID-THEFT (438-4338), TTY: 1-866-653-4261 or write to the Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580. If you have additional information or problems, call the hotline to update your complaint.

- You may also consider contacting other agencies for other types of identity theft.
  - The Social Security Administration if you think someone is fraudulently using your number (call (800) 269-0271 to report the fraud).
  - The Internal Revenue Service should be contacted if you suspect improper use of your personal identification information in connection with any tax abuse.
  - Lastly, contact your local Postal Inspection Service if you suspect that someone has submitted a change-of-address form in your name with intentions to redirect your mail or has used the mail to commit frauds connected to your identity.

Conclusion

Remember that identity thieves do not discriminate. Take precautions to protect yourself from becoming a victim. According to the Federal Trade Commission, once you realize that your identity has been stolen, there are five important steps you need to take:

Step 1: Immediately place a fraud alert on your credit reports by calling any one of the three nationwide credit reporting companies:

- Equifax: 1 (888) 378-4329
- Experian: 1 (888) 397-3742
- TransUnion: 1 (833) 395-6938

Step 2: Order and review your credit report carefully for any fraudulent activity or transactions that you are not aware of.

Step 3: Immediately close all accounts that have been tampered with or opened without your consent.

Step 4: Before reporting that you are a victim of identity theft to the Federal Trade Commission, file a local police report.

Step 5: Contact the Federal Trade Commission so they can investigate your identity theft case.

Resources

For more information about identity theft, contact or check the websites of the following:

- Consumer Action.
- Federal Trade Commission.
- Federal Trade Commission Identity Theft.
- Identity Theft Hotline at (877) 438-4338.
- USA.gov.
- AnnualCreditReport.com or call (877) 322-8228 for a free copy of your credit report. You are entitled to a free report from Equifax, Experian, and TransUnion.
- BBB Hotline at (903) 581-8373 or BBB Scam Tracker to report fraudulent activity or unscrupulous business practices.

References

- Alex Thomas Sadler, "There's a new victim of identity theft every two seconds: Here's the best way to protect yourself online," accessed October 16, 2021
- Federal Trade Commission, "What to Know About Tax Identity Theft," accessed October 16, 2021.
- Federal Trade Commission, "What to Know About Identity Theft ID Theft & Account Fraud: Prevention and Cleanup," accessed October 16, 2021.
- Federal Trade Commission, "Recovering from I.D. Theft," accessed October 16, 2021.
- Federal Trade Commission, "How to Protect Your Child from Identity Theft," accessed November 1, 2021.
- I.D. Watchdog from Equifax, "11 Ways Identity Theft Can Happen," accessed October 16, 2021.
- Identity Force: A Sontiq Brand, "Identity Theft by the Numbers," accessed October 16, 2021.
- Insurance Information Institute, "Facts + Statistics: Identity Theft and Cybercrime," accessed November 1, 2021.
- Internal Revenue Service (IRS), "Know the Signs of Identity Theft," accessed November 1, 2021.
- Internal Revenue Service (IRS), "Taxpayer Guide to Identity Theft," accessed October 16, 2021.
- Life Lock by Norton, "Why Teens Are at Risk for Identity Theft," accessed October 16, 2021.
- NerdWallet, Identity Theft: What It Is, How to Prevent It, Warning Signs and Tips, accessed October 16, 2021.
- Review 42, "How Many People Are Affected by Identity Theft?" accessed October 16, 2021.
- Tableau.com. COVID-19 and Stimulus Reports by Federal Trade Commission
- Total Identity Fraud Losses Soar to $56 Billion in 2020
- Yahoo Finance. U.S. lost about $200 billion due to fraudulent unemployment claims during pandemic: expert

Patricia Smith, *Human Sciences Regional Extension Agent*, Financial Resource Management and Workforce Development, Auburn University

For more information, contact your county Extension office. Visit www.aces.edu/directory.

New January 2022, FCS-2638