How to Avoid Identity Theft

If you would like, print this study aid for future reference.

Identity theft occurs when thieves steal your personal information (for example, your Social Security number (SSN), birth date, or credit card numbers). With sufficient information, another person can become you and use your identity to commit fraud or other crimes.

1. **Protect your SSN, credit card and debit card numbers, personal identification numbers (PINs), passwords, and other personal information.**
   Never provide this information in response to an unwanted phone call, fax, letter, or email, no matter how friendly or official the circumstances may appear. Be mindful of those who may be shoulder surfing (or trying to look over your shoulder) while you use the ATM, and seeking to steal your PIN. In case your wallet is lost or stolen, carry only the personal information you really need: checks, credit cards, or debit cards. Keep the rest, including your Social Security card, in a safe place. Do not preprint your SSN, phone number, or driver's license number on your checks. You have the right to refuse requests for your SSN from merchants. Ask the merchant to use another form of identification that does not include your SSN (like a passport) and have your driver's license number changed.

2. **Protect your incoming and outgoing mail.**
   For incoming mail: Try to use a locked mailbox or other secure location (for example, a post office box). If your mailbox is not locked or in a secure location, try to promptly remove mail that has been delivered or move the mailbox to a safer place. When ordering new checks, ask about having the checks delivered to your bank branch instead of having them mailed to your home where you run the risk of a thief finding them outside your front door.

   For outgoing mail containing a check or personal information: Try to deposit it in a United States (U.S.) Postal Service blue collection box, hand it to a mail carrier, or take it to the post office instead of leaving it in your doorway or home mailbox. A mailbox that holds your outgoing bills is a prime target for thieves who cruise neighborhoods looking for account information. Avoid putting up the flag on a mailbox to indicate that outgoing mail is waiting.

3. **Sign up for direct deposit.**
   Sign up for direct deposit of your paycheck or state or federal benefits, (like, Social Security). Direct deposit prevents someone from stealing a check out of your mailbox and forging your signature to access your money. It is also beneficial in the event of a natural disaster.

4. **Keep your financial trash "clean."**
   Thieves known as dumpster divers pick through garbage looking for pieces of paper containing SSNs, bank account information, and other details they can use to commit fraud. What is your best protection against dumpster divers? Before tossing out these items, destroy them, preferably using a crosscut shredder that turns paper into confetti that cannot be easily reconstructed.

5. **Keep a close watch on your bank account statements and credit card bills.**
   Monitor these statements each month and contact your financial institution immediately if there is a discrepancy in your records or if you notice something suspicious (for example, a missing payment or an unauthorized withdrawal). Contact your institution if a bank statement or credit card bill does not arrive on time. Missing financially related mail could be a sign someone has stolen your mail and/or account information, and may have changed your mailing address to run up big bills in your name from another location.

6. **Avoid identity theft on the Internet.**
   Never provide bank account or other personal information in response to an unsolicited email, or when visiting a website that does not explain how personal information will be protected. Legitimate organizations would not ask you for these details because they already have the necessary information, or can obtain it in other ways. If you believe the email is fraudulent, consider bringing it to the attention of the Federal Trade Commission (FTC). If you do open and respond to a phony email, contact your financial institution immediately. For more about avoiding phishing scams, or to obtain a brochure with tips on avoiding identity theft, visit www.fdic.gov.

   Take precautions with your personal computer (PC). For example, install a free or low-cost firewall to stop intruders from gaining remote access to your PC. Download and frequently update security patches offered by your operating system and software vendors to correct weaknesses that a hacker might exploit. Use passwords that will be hard for hackers to guess. For example, use a mix of numbers, symbols, and letters instead of easily guessed words. Also, shut down your PC when you are not using it. For practical tips to help you guard against Internet fraud, secure your computer, and protect your personal information, visit www.OnGuardOnline.gov.

7. **Review your credit record annually and report fraudulent activity.**
   Review your credit report carefully for warning signs of actual or potential identity theft (for example, items that include mention of a credit card, loan, or lease you never signed up for, and requests for a copy of your credit record from someone you do not recognize), which could be a sign that a con artist is snooping around for personal information. Learn more by visiting the FTC at www.ftc.gov/credit.

8. Get more information.
Visit the FTC at www.ftc.gov/idtheft or call **1-877-IDTHEFT (438-4338).**