Tips to Avoiding Identity Theft

In This Article
- Ways to stay safe at the bank, mailbox and more
- Don’t respond to calls or emails asking for personal information
- Beware of eavesdroppers in public places

In recent years, identity theft has received almost as much publicity as Britney Spears. Businesses nationwide have jumped on the bandwagon, marketing identity theft-related products like nobody’s business, and identity fraud insurance and credit monitoring products are springing up faster than crabgrass.

But, is all this really necessary? Has the country become overly paranoid about identity theft?

According to the Federal Trade Commission’s 2010 Javelin Identity Fraud Survey Report, this “paranoia” is justified. Because of identity theft:

- 8% of people first discovered they were a victim when they were contacted by a debt collector.
- Consumer costs for medical fraud results in an average of $18,480.

An estimated 11.1 million consumers are victimized annually. In worst-case scenarios, victims might lose job opportunities, loans, or have arrest warrants issued due to an identity impersonator.

Paranoid? Not likely. Any steps you take to combat identity theft make you a prepared, responsible consumer who would rather be safe than sorry.

Your Identity Theft Protection Checklist
- Adopt a need-to-know approach to your Social Security number and mother’s maiden name. If a business asks for this information, ask what it will do with the information, why the company needs it, how the company will protect it, and what will happen if you refuse to provide this information.

- Never carry your Social Security card, birth certificate, checks, credit cards, or passports unless you need them.

- Shred or hide all documents (credit card statements, bills, credit card receipts, tax returns, unused checks, canceled checks, and credit reports) that contain account information, Social Security numbers, PINs, or sensitive information. Also shred or otherwise destroy expired credit cards and driver’s licenses, and never leave receipts at bank machines, bank counters, trash receptacles, or unattended gas pumps.
✓ Check your credit report at least quarterly. If you are planning to make a major purchase that will require a credit check, check your credit report monthly.

✓ Consider enrolling in an identity theft protection product, such as ProtectMyID™, which will monitor your personal information and alert you to key changes. ProtectMyID also offers a $1 Million Product Guarantee.

✓ Inspect credit card bills, telephone bills, and bank statements for unauthorized use.
✓ Keep your wallet and purse hidden from guests, employees, and coworkers.

✓ Keep your computer files locked and password-protected.
  o When not in use, log off your computer.
  o Create a separate account for each user and do not share your computer login passwords with anyone (with the exception of a trusted spouse or computer administrator).

✓ Do not use public or work computers to access bank accounts or other personal accounts.

✓ Never send personal information via email, and never respond to emails asking you to verify your password, account number, Social Security number, or credit card numbers.

✓ Install antivirus software, anti-spyware, and firewall software to prevent cyber-programs that steal personal information.

✓ Consult with a network professional to make sure your computer system is secure.

✓ When paying by credit card, keep your credit card within sight at all times to avoid “skimming,” which occurs when a worker swipes your credit card into a portable electronic device that gathers all the personal information the card contains.

✓ Use ATMs located at major banks only. Never use ATMs that have evidence of tampering, and be cautious of people who might be able to see your card account number or PIN.

✓ Be secretive about your passwords and PINs.
  o Use passwords that are at least six digits and include letters, numbers, symbols, and upper and lower cases.
  o Choose different passwords and PINs for each account.
  o Do not choose obvious passwords. Avoid pets’ names, birthdates, or last four digits of your phone number or Social Security number.
  o Change passwords regularly.
  o Memorize passwords instead of writing them down.
  o Do not give passwords or PINs to other people.
✓ Do not respond to incoming phone calls requesting personal information. If a creditor or organization calls with a legitimate need for your personal information (account numbers, Social Security number, or credit card information), hang up and verify the phone number and legitimacy of the caller before returning the call.

✓ When giving vendors your credit card number, Social Security number, or other personal information via telephone, make sure no eavesdroppers can overhear the conversation.

✓ Opt out of the mailing lists for pre-approved credit card offers by calling 1-888-567-8688.

✓ Open all bills and bank statements promptly and reconcile all accounts monthly.

✓ Notify your creditors before you move.

✓ Never use open mailboxes to send or receive mail. Instead, use locked mailboxes or United States Postal Service mailboxes.

✓ When on vacation, ask the post office to place a vacation hold on all mail.

✓ Keep a schedule that indicates when credit card bills, bank statements, new credit cards, and other mail is scheduled to arrive, and contact all relevant creditors, banks, or vendors if an expected piece of mail is late.

✓ Never send new checks to a mailbox, secured or not. Instead, ask the issuing bank to hold the checks at the branch.

✓ Never mail anything with your account number printed on the outside of the envelope.

✓ When shopping online, follow two rules:
  1. Purchase only from reputable companies and confirm that sites are secure before placing an online order. Look for the closed lock icon to appear at the bottom of your browser to check the website’s security status. Also check the site’s privacy policies to make sure they are not distributing or selling your name and information without your permission.

  2. Do not save or “remember” credit card information or passwords with websites. Even reputable companies have security breaches.

✓ Order your Social Security Earnings and Benefits Statement annually to check for fraud by calling 1-800-772-1213.

Copyright 2010, ProtectMyID™. All rights reserved.