



Avoiding Identity Theft: Steps You Can Take Right Now to Protect Yourself

Avoiding Identity Theft: Steps You Can Take Right Now to Protect Yourself

Identity theft occurs when someone obtains important personal information and uses it without your permission to commit fraud or theft. Today's identity thieves are information seekers, and they don't need to steal your wallet. They obtain bits of information by sorting through trash for discarded receipts and statements, spying for your PIN number at ATM machines or telephone booths, accessing public records and even stealing items from your mail box.

This guide contains what we believe to be current best practices. The information we have provided should help minimize the chance that you will become a victim of identity theft. Links to additional information are provided in this guide for your reference.

Step 1: Minimize Information Access

Step 2: Smart Use of Credit Cards

Step 3: Protect Passwords and PINs

Step 4: Online Safety

Step 5: Research Additional Online Information

Section 1: Minimize the amount of information that can be accessed

1. Clean out your wallet and purse, and carry only what you need. Do not routinely carry all your credit cards, your Social Security card, birth certificate, or passport.
2. Remove your name from the marketing lists of the three credit bureaus. You can do this by calling 1-888-567-8688. This will significantly reduce the number of pre-approved offers you receive in the mail. When in transit or tossed into the trash, these credit card solicitations can be used by identity thieves who use them to order credit cards in your name.
3. Order your credit report once a year from each of the three credit bureaus to check for inaccuracies and fraudulent use of your accounts. The three credit reporting agencies have authorized Annualcreditreport.com (1-877-322-8228) as the official site to distribute free credit reports. (If you go directly to the individual credit reporting agencies, you will be charged unless you fit other criteria for a free report) The agencies have stressed that this is the only web site they have endorsed to distribute free annual reports. Other web sites offer credit reports, but if you read the fine print, many of them sell your information to third parties. Help prevent the distribution of your personal information by calling 877-322-8228 or utilizing the officially sanctioned site: Annualcreditreport.com .

HINT It's suggested that you request a report every four months from one of the three agencies. This provides you with the ability to monitor your credit report three times a year at no charge. Monitoring your credit report, credit card statements, and bank statements is the most important step you can take to safeguard your credit record.
4. Remove your name and address from the telephone book. The information in telephone books is often utilized to set up online directories that are accessed by identity thieves. In addition, these directories often interface with online mapping services which make it easy for people to obtain a map to your home. By eliminating public access to your address and phone number, you can help protect your personal information from telemarketers and identity thieves.
5. Decrease spam and minimize the possibility you'll receive a phishing e-mail by limiting where your e-mail address is used. Here are some of the ways in which spammers can access your e-mail address: newsgroup postings, chat rooms, websites, online service's membership directories or profiles, purchased lists from legitimate businesses, "chain letter" e-mail messages, online yellow and white pages, and address books and e-mail on other people's computers infected with a virus.
6. Think twice before disclosing the Social Security number of anyone in your family. This includes doctor's offices, financial institutions, and other organizations. Question why they are requesting it. Often a Social Security number is solicited on a routine basis, although there is no legitimate need for it. Your Social Security number is the key to your banking and credit card accounts, insurance and health benefits, making it a prime target of identity thieves. Ask if there are alternative numbers that can be used in place of a social security number.
7. Children and infants are the latest victims of identity theft, because their stolen identification can go unnoticed for years. Only give your child's social security number (SSN) when absolutely necessary. If someone asks for a SSN for general record keeping you have the right to refuse. Offer other types of identifying information whenever possible. Never carry your child's SSN card with you; always store it in a secure place. The three credit reporting agencies (Equifax, Transunion and Experian) do not recommend that you automatically check your child's credit report annually UNLESS you have some reason to believe there is a problem. A child should not automatically have a credit file unless someone has started to apply for credit using that child's Social Security number.

8. Consider installing a locked mail box at your residence to reduce mail theft, or use a post office box.
9. When ordering new checks, consider removing information such as your Social Security Number, driver's license number, middle name, and telephone number. The less personal identifying information you make available, the more likely an identity thief will choose an easier target. Do not have new checks sent to your house. Request to pick them up at the bank.
10. Store new checks, canceled checks, and any statements you receive in a safe place. In the wrong hands, they could reveal a lot of information about you, including your account numbers, telephone numbers, and driver's license number.
11. "Dumpster divers" look through trash for information they can use to steal your identity. Always shred sensitive information like credit card receipts, banking statements, phone bills, and so on. Home shredders can be purchased in most office supply stores.
12. Cordless and cellular analog telephones are not well encrypted, and it's easy for others to listen to your calls with simple scanners that are readily available at most electronic stores. Therefore, when talking on an analog cordless or cellular telephone never give out private personal data. A "land line" (conventional non-wireless telephone connection) makes it significantly more difficult for someone to listen to your telephone conversations.

Section 2: Smart Use of Credit Cards

1. Carry only one or two cards in your wallet; you don't need to carry every card you own. Also, consider minimizing the number of cards you use, and canceling any unused credit cards. Although you don't use them, the account numbers are listed in your credit report, which is full of information that can be used by identity thieves.
2. Keep a list of all your credit card account numbers and expiration dates. It's also important that you know the telephone numbers of the customer service and fraud departments for every card. You can easily document this information by photo copying the front and back of all your cards. Keep this information in a secure place so you can contact the credit card companies if your cards are lost or stolen. Do the same with your bank accounts.
3. Never give out your credit card number or other personal information over the telephone unless you have a trusted business relationship with the company AND YOU HAVE INITIATED THE CALL. Identity thieves often call their victims with a story that sounds very legitimate. Hang up and call the company to determine if phone call is legitimate. Obtain the telephone number listed in the phone directory, or on a recent statement you received. Don't call a number given to you by the person who initiated the call.
4. Don't throw credit card or ATM receipts into a public trash container or leave them at a place of business. Always take them with you.
5. Watch the mail when you are expecting: 1- a new credit card you have applied for, or 2- a reissued credit card that has expired. Contact the credit card company immediately if the card does not arrive.
6. If you receive convenience checks from credit card companies always shred them. Never throw them in the trash or recycling bin without shredding them first. They are easy for identity thieves to steal and use while the consumer is unaware that the checks were even issued.
7. Request, in writing, that each credit card issuer removes your name from their marketing and promotional lists. They may sell or share this information with other companies. You will need to contact the issuer to obtain the mailing address for this request. You won't send this to the same address you use when mailing in your payments.
8. Be very careful before you use a credit card on the Internet, or provide personal information (such as your Social Security number or birth date) on an electronic application. Make sure the Internet site is managed by a reputable company, and the pages requesting personal information are encrypted. Research your purchase options online, and consider placing your order by phone if this is an alternative.
9. One of the best things you can do to protect your accounts is to obtain online access, and review transactions that are posted each day. There's no need to wait for your monthly statement to examine account activity. Online access lets you review transactions daily so you can make sure they are generated by you or another individual listed on the account. At least once a week, review your credit card statements and bank account information (as well as all bills) for unauthorized charges or fraudulent use.

Section 3: Protect Passwords and Personal Identification Numbers

1. The simpler a password format is, the easier it is for someone to figure out. When creating passwords and PINs, do not use the last four digits of your Social Security number, your birth date, middle name, mother's maiden name, pet's name, address, consecutive numbers, or anything else that could be discovered easily by thieves.
2. The importance of picking a good, secure password can't be emphasized enough. Because passwords and PINs are there for your protection, you don't want to pick something that can be guessed by others. One of the primary ways people gain unauthorized access to a password-protected system is by guessing passwords.

The following guidelines will guard against someone finding out your password and using your account illegally:

- The best passwords are at least 8 characters in length and use a combination of numbers, special characters, and upper- and lower-case letters. The longer your password is, the longer it will take someone (or more likely, some program) to crack it.
- Do not use personal information in your password that someone else is likely to be able to figure out. Obviously, things like your name, phone number, address, birth date, etc. are to be avoided.
- Do not use words, geographical names, or biographical names that are listed in standard dictionaries.
- Never use a password that is the same as your account number.
- Do not use passwords that are easy to spot while you're typing them in. Passwords like 12345, or nnnnnn should be avoided.
- Do not write your password anywhere. A password you write down is as good as having no password at all. Choose a password you can memorize but follows the guidelines above
- Change your passwords often. This includes sites you access for financial information, e-mail, shopping, etc. It's also important that you don't use the same password for every site you access.
- Use your hand to shield the key pad when using your PIN at a bank ATM or when making long distance phone calls with your phone card. "Shoulder surfers" may be spying nearby with binoculars or a video camera.

Section 4: Online Safety

1. Microsoft and Apple regularly release patches for their operations systems. Regularly check for updates to the application you use and install them. Keeping your applications updated is important.
2. When using a public computer, do not input personal information, usernames or passwords. There's no way to know how the computer's preferences have been set up, or if the computer has been infected with a virus or spy ware. When using a public computer, assume that everyone can see everything you are doing.
3. If you get an email or pop-up message that asks for personal or financial information, do not reply, and never click on a link in the message. Legitimate companies don't ask for this information via email. If you are concerned about your account, contact the organization mentioned in the email using a telephone number you know to be genuine, or open a new Internet browser session and type in the company's correct Web address yourself. It's important that you don't cut and paste the link from the message into your Internet browser. Thieves can make links look like they go to one place, but that actually send you to a different site.
4. If you access the Internet by cable or broadband, it's critical that you use a firewall. A personal computer connected to the Internet without a firewall can be hijacked in just a few minutes. An Internet firewall is a piece of software or hardware that helps screen out hackers, viruses, and worms that try to reach your computer over the Internet. If you are a home user or small-business user, installing a firewall is the most effective and important first step you can take to help protect your computer. It is important to have a firewall and antivirus software turned on before you connect to the Internet. Most broadband routers have built-in firewalls, and users should check their documentation to see if theirs does.
5. Wireless Internet access offers convenience; however, unless you take certain precautions, anyone with a wireless-ready computer can use your network and potentially access the information on your computer. Wireless networks have spawned a new past-time among hobbyists and corporate spies called war-driving. The data voyeur drives around a neighborhood or office district using a laptop and free software to locate unsecured wireless networks in the vicinity, usually within 100 yards of the source. The laptop captures the data that is transmitted to and from the network's computers and printers. The data could include anything from one's household finances to business secrets.

Fortunately, there are steps you can take to protect your wireless network and the computers on it:

- Use encryption.
- Use anti-virus and anti-spyware software, and a firewall.
- Turn off identifier broadcasting. Change the identifier on your router from the default.
- Change your router's pre-set administration password.
- Designate only specific computers to access your wireless network.
- Turn off your wireless network when you aren't using it.
- Don't assume public places with wireless connectivity are secure.
- Be careful about the information you access or send from a public wireless network.

Remember, wireless data networks are in their infancy. To ensure that your system is secure, review your user's manuals and web resources for information on security. Two useful guides can be found on the web at www.practicallynetworked.com/support/wireless_secure.htm and at www.csrc.nist.gov/publications/nistpubs/800-48/NIST_SP_800-48.pdf

6. Spyware is software installed on your computer without your consent to monitor your computer use. Clues that spyware might be on a computer include a deluge of pop-up ads, a browser that takes you to sites you don't want, unexpected toolbars or icons on your computer screen, keys that don't work, random error messages, and sluggish performance when opening or saving files. There are steps you can take to help lower your risk of spyware infections:
 - Update your operating system and Internet browser software, and set your browser security high enough to detect unauthorized downloads.
 - Use anti-virus and anti-spyware software, as well as a firewall, and update them all regularly.
 - Download free software only from sites you know and trust. Enticing free software downloads that frequently bundle other software, including spyware.
 - Don't click on links inside pop-up windows.
 - Don't click on links in e-mail or pop-ups that claim to offer anti-spyware software; you may unintentionally be installing spyware.

Step 5: Research Additional Online Information

This document contains what we believe to be current best practices, but there are additional information sources you might consider accessing. We have listed a few resources below; however, there are many available. When researching information online it's critical that you access reputable sources. This will help you avoid scam artists who have a legitimate looking web site, but are waiting to take advantage of individuals who are seeking information on identity theft and fraud.

1st Source Bank Infosource:

<https://www.1stsource.com/infosourceonline/index.jsp>

Experian:

<http://www.experian.com/>

Equifax:

<http://equifax.com/>

Trans Union:

<http://www.transunion.com/index.jsp>

Free Credit Report – Sponsored site of the 3 reporting agencies:

<http://www.freecreditreport.com/>

Federal Trade Commission – National Resource for ID Theft:

<http://www.consumer.gov/idtheft/>

Social Security Online:

<http://www.ssa.gov/pubs/idtheft.htm>

Identity Theft Resource Center:

<http://www.idtheftcenter.org/alerts.shtml>

Privacy Rights Clearinghouse

<http://www.privacyrights.org>

Microsoft Security at Home

<http://www.microsoft.com/athome/security/default.mspix>