



8 easy ways to steal your identity (and how to prevent it)

Every day, we inadvertently do things that put our identity at risk. Declare your own personal war on identity theft by being aware of the risks and taking action to protect yourself from this invasive and time consuming crime. Here are the easy ways thieves can take your identity, and how to safeguard against theft:

1. **Unlocked mailbox** – Even though it's a felony to steal mail, thieves will take mail out of an unlocked box and gain a great deal of personal information. With identifying information such as account names and numbers, and employment history, thieves can open your pre-approved credit card accounts, commit bank, benefits or tax fraud. If possible, buy a mailbox with a lock on it, or create an opening so that mail goes directly into your house.
2. **Smart phone cameras** – Thieves can position themselves to hear or see your personal information while you're applying for credit or filling out a job application or medical forms. Smart phones can record your information while the person stealing it appears to be talking or texting. Be aware of your surroundings, do not say your personal information such as a social security number out loud, and create a private space for filling out paperwork.
3. **Trash that's treasure** – Unless you shred all documents that contain personal information, a thief looking through trash has easy access to documents such as bank account names and numbers. Buy a shredder – and use it.
4. **Stolen wallet** – It's an old-fashioned way of stealing, but very prevalent. Don't carry cards (especially a social security card) or information that you don't need regularly. And, make copies of the front and back of all cards in your wallet. Better yet, find a service that can handle the details quickly when you discover that your wallet or purse is stolen.
5. **Address change** – A thief will fill out a change of address form for your mail, re-routing your personal documents to another address. While this is one that is difficult to prevent, staying on top of your mail and what bills and checks to expect helps early detection.
6. **File sharing** – When you share music, photos or videos on a peer-to-peer network, information stored on your hard drive is vulnerable. Others with whom you share music or video files can download your personal files as well, such as tax returns or password documents. Beware of file sharing on a computer that contains sensitive documents. You may want to export your personal documents to store offline except when needed.
7. **Online shopping** – Thieves are good at duplicating legitimate online shopping venues. You may click through to an online shopping site from an email or an online ad. Then, thinking you're in the legitimate store, give your personal information and credit card access to a fraudulent site set up for identity theft. Instead of clicking through on an email or ad, type the address of the online store directly into your Web browser. Be sure you logout of a site before closing the window.

8. **Phishing (email), SMSishing (text) and Vishing (voice calls)** – Illegitimate requests for your personal information come from many sources. Don't respond to claims that your account numbers or passwords need to be verified. If you think a request may be valid, initiate the call yourself to a phone number provided by your financial institution, not the requesting party.

Unfortunately, you may not be aware of fraud that comes from data breaches at otherwise secure facilities or an overlay or skimmer that is placed by thieves on credit/debit card card slots. Watch your bills and bank accounts for activity that is suspicious, and report inconsistencies right away to your financial institution.