

## Your 5-minute guide to protecting your identity

Here are 16 steps to protect yourself and six ways to clean up things if you are a victim of identity theft.

Thieves may sell your information on the black market or use it to obtain money, credit or even expensive medical procedures. Unless you're vigilant in protecting your records, you'll have to work even harder to repair the damage to your credit. The average victim spends 30 to 40 hours rectifying the problem.

Some of the e-threats to your identity are:

- **Phishing.** You get an e-mail that appears to be from your bank or an online service, most often PayPal or eBay, instructing you to click on a link and provide information to verify your account.
- **Pharming or spoofing.** Hackers redirect a legitimate Web site's traffic to an impostor site, where you'll be asked to provide confidential information.
- **Smishing.** This is phishing done with text messaging on your smart phone. It instructs you to visit a bogus Web site.
- **Spyware.** You've unknowingly downloaded illicit software when you've opened an attachment, clicked on a pop-up or downloaded a song or a game. Criminals can use spyware to record your keystrokes and obtain credit card numbers, bank-account information and passwords when you make purchases or conduct other business online. They also can access confidential information on your hard drive.

You don't need to have a computer to become a victim.

- **Vishing -- voice phishing.** You get an automated phone message asking you to call your bank or credit card company. Even your caller ID is fooled. You call the number and are asked to punch in your account number, PIN or other personal information. (See ["Your phone may be under attack."](#))
- **Bank-card "skimming."** Crooks use a combination of a fake ATM slot and cameras to record your account information and PIN when you use a cash machine. Your credit or debit card also can be skimmed by a dishonest store or restaurant worker armed with a portable card reader. (See ["Is your waiter a thief?"](#))
- **Crooks will steal your wallet** or go through your mail or trash.

More than half of identity theft cases involve credit card fraud. Checking accounts are the second most popular target. But some crooks have other plans:

- At least 250,000 people have been the victim of medical identity theft in the last several years. (See ["Diagnosis: Identity theft."](#)) Crooks use fraudulently obtained personal information to get expensive medical procedures or dupe insurance companies into paying for procedures that were not done.
- The victims of about 5% of reported identity theft cases are children. The fraud often goes undetected for years -- until the young adult applies for credit. (See ["Stolen innocence: Child identity theft."](#))

### 16 tips to protect yourself

You can take steps to protect yourself from identity fraud:

- Keep your confidential information private. Your bank or credit card company won't call or e-mail to ask for your account information. They already have it.
- Keep an inventory of everything in your wallet and your PDA, including account numbers. Don't keep your Social Security card in your wallet.
- Stop getting banking and credit card information in the mail. (See "[Go paperless for safer banking.](#)")
- Monitor your bank and credit card transactions for unauthorized use. Crooks with your account numbers usually start small to see if you'll notice.
- If you conduct business online, use your own computer. A public computer is less secure, as is wireless Internet.
- Look for suspicious devices and don't let anyone stand nearby when you use an ATM. Take your card and receipt with you. Keep your PIN in your head, not in your wallet.
- Don't store credit card numbers and other financial information on your cell phone. (See "[Is your cell phone spilling your secrets?](#)")

Protect your computer from vulnerability:

- Install anti-virus, anti-spyware and firewall protection, and keep them up to date.
- Don't open e-mails from strangers. Malware can be hidden in embedded attachments and graphics files.
- Don't open attachments unless you know who sent them and what they contain. Never open executable attachments. Configure Windows so that the file extensions of known file types are not hidden.
- Don't click on pop-ups. Configure Windows or your Web browser to block them.
- Don't provide your credit card number online unless you are making a purchase from a Web site you trust. Reputable sites will always direct you to a secure page with an URL starting with *https://* whenever you actually make purchases or are asked to provide confidential information.
- Use strong passwords: at least six characters, including at least one symbol and number, and no reference to your name or other personal information. Use a different password for every site that requires one, and change passwords regularly.
- Never send a user name, password or other confidential information via e-mail.
- Consider turning off your computer when you're not using it or at least putting it in standby mode.
- Don't keep passwords, tax returns or other financial information on your hard drive.

## 6 steps to clean up the mess

If you suspect your identity may be compromised, place a fraud alert with the three credit bureaus. When you place an alert, you are entitled to a free copy of your credit report. After that, take advantage of the free annual reports the bureaus are required to give all consumers. Stagger your requests so that you get a report every four months.

- If you've been phished, contact the bank or company named in the fraudulent e-mail. You also may want to notify the [Internet Crime Complaint Center](#) and forward the e-mail to [spam@uce.gov](mailto:spam@uce.gov).

If you are the victim of identity theft, take the following steps:

- Make an identity-theft report to the police and get a copy. File a complaint with the [Federal Trade Commission](#). Also, contact the office of your state's attorney general; you may be able to file a report there.
- Close accounts that have been tampered with. Contact each company by phone and again by certified letter. Make sure the company notifies you in writing that the disputed charges have been erased. Document each conversation and keep all records.
- Place a seven-year fraud alert or a "freeze" on your credit reports. (See "[Lock your credit away from ID thieves](#).")
- Begin the process of having the fraudulent information removed from your credit reports. (See "[Don't let credit-report errors fester](#).")
- Find victim support at the [Identity Theft Resource Center](#).