

By Debra Littlejohn Shinder, MCSE, MVP

Identity theft, which involves using another person's credentials and personal information (name, address, social security number, driver's license number, credit card and bank account numbers, etc.), is one of the fastest-growing crimes in today's information-laden world. ID thieves usually use this information to access the victim's money, obtain property fraudulently in the victim's name, or distinguish the thief's own identity when committing other crimes.

According to statistics from the Federal Trade Commission's January 2006 report, the organization received more than 685,000 complaints of consumer fraud last year, with 37 percent representing cases of ID theft. Estimates of the true number of cases is much higher; fightidentitytheft.com estimates that 10 million Americans have already been victimized, at a total cost of more than \$50 billion.

Luckily, there are things you can do to avoid becoming one of these statistics, as well as ways to minimize the damage if you do become the target of an ID thief.

1 Shop only secure sites

Some people think buying things online puts them at inordinate risk of identity theft—yet those same people think nothing of allowing a waiter or retail store clerk to whisk their credit card away to some back office where they could easily record the numbers and information or even make a "white card" copy of its magnetic strip. The key to safe online financial transactions is to shop only at reputable Web sites and to be sure transactions are secured with SSL encryption (which you can recognize by the little "locked" icon at the bottom of most Web browsers).

One caveat, though: You want to deal with sites that use encryption so someone can't steal your payment information as it passes across the Internet—but scam sites can encrypt their transactions too. So we're back to the basic: Buying from Amazon.com or the Microsoft Web site is safer than ordering from Joe's Homepage (unless you know who Joe is and that he can be trusted).

2 Protect your personal information

Online or off, it's not just your credit card numbers that you need to guard diligently. In some cases, just a name is enough for an ID thief to gather much more information about you. If you have a name that's common, like John Smith, it won't be so easy, but if your name is unusual, so that you're the only one with that name in your particular city or region, an ID thief may be able to find out your address, phone number, and date of birth through an online "people search" service, such as Zabasearch. Then with *that* information, if you own your home and live in a county that puts its property records on the Web, the thief can go to that site and find out how much your home is worth, getting a good idea of whether you're a good target. Some tax districts even include a photo of your home, which may show your car sitting in the driveway with license plate number displayed. Be aware of your online presence and opt out of as many directories and databases as possible.

3 Protect PINs and passwords

Make sure you have strong passwords for your online banking services, electronic bill-paying, and other financial accounts. Don't use easily discovered passwords such as your mother's maiden name, your social security number, or your birth date. A good password is long (at least eight characters; 14 is better) and complex, containing a mixture of upper- and lowercase alphabetic characters, numeric digits, and symbols and not containing any words found in the dictionary. PINs are often limited to four numeric digits. If you have a choice in creating the PIN, make sure the numbers are random and not easy to guess (for example, don't use your street number or the last four digits of your SSN).

It goes without saying that you shouldn't write down your passwords and PINs, and you should never share them with anyone else. If it's absolutely necessary to do so (for example, in an emergency situation where you need a friend to withdraw money from an ATM with your card), change the password or PIN immediately afterward.

4 Protect sensitive data on your computer

If you have any personal or financial information stored on your computer, use Windows EFS or a third-party encryption program to protect it. Update your virus software regularly and use a firewall to prevent intrusions. Keep your operating system and applications updated, especially with critical security patches. Use an anti-spyware program. Don't use file-sharing programs or visit Web sites that are more likely to contain dangerous code, such as hacker sites, porn sites or warez (pirated software) sites. Don't open attachments from people you don't trust and don't click on links in strangers' e-mail messages.

Don't put sensitive information on laptops, handheld computers, or other portable devices unless absolutely necessary. If you need to access such data while on the go, store it on a flash drive or memory card and carry the storage device separately from the computer. Don't set your computer up to log automatically, especially portable computers.

If you sell or give away an old computer, first use an overwriting program to get rid of the information on the drive (just deleting or even formatting is not enough), or even better, remove and destroy the hard disk and let the new owner install another one.

5 Use an alternate identity for casual Web surfing

Many savvy Internet users have learned that it's smart to have multiple e-mail addresses and to use an alternate (for example, an account with a Web mail service such as Hotmail, Yahoo, or Gmail) when you need to enter information to access a site. If you're just casually surfing and not conducting business, there's no reason to give any site your real e-mail address or even your real name, address, and other personal information.

Some sites require you to register (at no charge) to access or post to the site. And some of these sites sell the lists of registered users for marketing purposes. An identity thief can easily pose as an advertiser and buy the same list. Having several alternate identities can help you track down what sites are selling your info. For example, Jeff might use the name Jeff Johns when he registers on a site called John's Fishing Gear, and the name Jeff Booker when he registers on a site called the Big Book Place, and use e-mail addresses associated with those names (jjohns@gmail.com and jbooker@hotmail.com, for example). Now when he starts getting tons of spam addressed to his jbooker account, he knows the Big Book Place is the one who sold his info.

6 Learn to recognize phishing scams

Phishing e-mails are a particularly insidious form of spam. It's annoying enough to have your mailbox fill up with junk mail from legitimate companies, but phishers aren't really selling anything; they're just "phishing" for your credit or debit card information or bank account numbers, or other personal information they can use.

A good example is the ever-popular "You qualify for low rates on home refinancing." The scam site isn't a mortgage company, but its Web site is set up to make you think it is. When you fill out the detailed loan application, you give the phisher a wealth of information that includes your social security number, banking information, income, employers, present and former addresses, relatives and friends' names and addresses, and much more that can be used to impersonate you successfully.

Other examples of phishing messages include those purporting to be from your bank or credit card company or a legitimate site with which you do business, such as eBay, notifying you that you must click a link to update your account information. Many even claim they're asking you to do this to prevent your account from being closed or used fraudulently.

Phishing messages can often be detected by the fact that links go to a different URL from the one that appears in the message. For example, if you hover over "www.ebay.com" in the message, you might see that the hyperlink actually takes you to www.scammersite.com/ebay. A good rule of thumb is to never respond to any e-mail message asking you to return personal information. Instead, call or write directly to the company that the message purports to be from.

7 Use cash or credit

There are lots of ways to pay for your purchases these days, but some are safer than others. When it comes to protecting your identity, good old-fashioned cash is still king. Unfortunately, there's no way yet to insert a twenty dollar bill into a slot in your computer to make a purchase.

Often, you have the choice to pay for online purchases by credit card, debit card, electronic check, or direct bank account withdrawal. All of these require you to submit precious information that an ID thief would love to get hold of. None of these types of information is more or less likely to be stolen, but there are a couple of advantages to paying by credit card. First, many sites require that when you pay by credit card, you enter the security code (the three-digit number on the back of your card). This adds a layer of protection, since a fraudster who obtained your credit card number from a receipt or other source would not know this number.

More important, if you *do* become a victim of credit card fraud, the law limits your liability to \$50. You don't have this protection with debit cards—they work like paying cash, in that once the money's gone, it's gone.

Checks also contain a huge amount of information for scammers: your name, address, and phone number, and many people have their driver's license number printed on the check. And of course your bank account number, the bank's routing numbers, etc., are also printed on the check. A clever scammer can create new checks on your account and forge your signature or use direct withdrawal to take money from your account.

8 Get off the lists

Keeping "preapproved" credit offers out of the hands of identity thieves by using safe mail management practices is good; stopping them from being sent to you altogether is even better. (After all, even if you use a PO box or locked mailbox, it's possible for a dishonest postal employee to intercept them.) You can contact the three major credit reporting bureaus ([Experian](#), [Equifax](#), and [Trans Union](#)) individually to have your name removed from their marketing lists. Or call 888-5OPTOUT (888-567-8688). This won't stop all the offers, but it will reduce the number.

9 Check your credit report

Identity theft can go undetected for a long time. Someone's out there, using your name and social security number to open credit accounts or apply for loans, but because he or she is diverting correspondence to a different address, you may not know until the collection agencies start hunting you down. By that time, thousands of dollars of charges may have accumulated. One way to keep an eye on what's going on with your account is to check your credit report regularly.

New federal laws require that the credit bureaus provide you with one free credit report each year. You can space them out, getting one from Experian in the spring, one from Trans Union in the summer, and one from Equifax in the fall, for example, to better monitor your credit activity without paying extra. Look for inquiries or new accounts you didn't authorize. The sooner you find out you're an ID theft victim, the easier it will be to repair the damage. You can also order free reports through www.annualcreditreport.com.

10 Report identity theft attempts

If you're a victim of identity theft, report it to your local police department. You may need a copy of the police report to submit to creditors as proof that you were a crime victim. Contact the fraud departments of the three credit bureaus and put a fraud alert on your account; this will require creditors to contact you before opening a new account in your name or making changes to your existing accounts (such as sending your bank statements to a new address). Close the accounts that have been compromised.

File a complaint with the Federal Trade Commission (FTC) to go into their database, which is used by law enforcement agencies in investigating ID theft. You can file this report [online](#).

Additional resources

- TechRepublic's [Downloads RSS Feed](#) **XML**
- Sign up for TechRepublic's [Downloads Weekly Update](#) newsletter
- Sign up for our [Network Security NetNote](#)
- Check out all of TechRepublic's [free newsletters](#)
- ["12 steps to avoid phishing scams"](#) (TechRepublic download)
- ["Educate your users about e-mail safety with this PowerPoint presentation"](#) (TechRepublic download)
- ["10 common social engineering ploys... and how to protect against them"](#) (TechRepublic download)

Version history

Version: 1.0

Published: May 10, 2006

Tell us what you think

TechRepublic downloads are designed to help you get your job done as painlessly and effectively as possible. Because we're continually looking for ways to improve the usefulness of these tools, we need your feedback. Please take a minute to [drop us a line](#) and tell us how well this download worked for you and offer your suggestions for improvement.

Thanks!

—The TechRepublic Downloads Team