

Be a Savvy Surfer; Protect Yourself from Cyber Thieves

If you give out personal information online without a thought, you might fall prey to an identity thief. Identity thieves use pieces of your personal information, such as your Social Security number (SSN) to commit fraud or theft, without your knowledge.

Perhaps the most common result of identity theft is that a thief will use your name and personal information to open a credit card account. After the thief wracks up dollars and dollars of debt, you're left with the wrecked credit history.

But, there are ways that you can take action against identity theft. Follow these simple steps.

The Federal Trade Commission (FTC) maintains a Web site dedicated to consumer protection against identity theft.

At the site, you can download copies of the guide *Identity Theft: When Bad Things Happen To Your Good Name*. The document includes tips for maintaining control of your identity while online and what to do if identity theft happens to you. To download the document, visit <http://www.consumer.gov/idtheft/>

Practice High-speed Internet Security

The Federal Trade Commission (FTC) has released a guide to safety for computers connected to the Internet at high speed called "Safe at Any Speed." The document explains the risks of computer viruses and hacking that come with a fixed IP address. "Safe at Any Speed" outlines steps consumers can take to protect their computers and data.

To access an electronic version of this document (text or pdf), visit the FTC Information Security Web site: <http://www.ftc.gov/bcp/online/edcams/infosecurity>.

Protect Your Property: Install a Firewall and Anti-virus Software

To guard against online intruders who may hi-jack your computer or possibly destroy your property via a computer virus, install a firewall and/or anti-virus software.

Remember to update your anti-virus software regularly. New viruses are created every day!

- **McAfee Security's** Security Service (<http://www.mcafee.com/>) combines one full year of coverage using their popular products:
 - VirusScan Online
 - Personal Firewall Plus
 - Privacy Service

- **Symantec's Norton Internet Security 2003** (<http://www.symantec.com/product/>) includes virus protection, a personal firewall, and privacy options.

FTC wants to help you reduce Spam

The Federal Trade Commission (FTC) wants to help reduce the amount of Spam that comes into your mailbox.

Even if you set Spam Detection and Spam Block, it's a good idea to follow the advice of the FTC. The tips provided below help reduce your exposure to Spam harvesters that collect e-mail addresses for online marketers.

- Avoid displaying your e-mail address in public spaces, including newsgroup postings or chat rooms, on Web sites, or in online directories.
- Check a Web site's privacy policy before submitting your e-mail address.
- Read the fine print on Web site forms before you transmit personal information. If possible, select the "opt-out" choice if the Web site plans to share your information.
- Create two e-mail addresses – one for personal messages and the other for public use, such as in newsgroups or chat rooms.
- Create a unique e-mail address. Spammers often use "dictionary attacks" to sort through possible name combinations at large Internet Service Providers (ISPs) or e-mail services to find valid addresses. So a common name, like "jdoe," may get more spam than a unique name, like "jd51x02oe."
- Use Spam Detection and Spam Block.
- Report the Spam to your ISP and to the sender's ISP. Often the e-mail address to report Spam is "abuse@[sender ISP's name].com." The ISP may be able to stop further Spam.
- Report the problem to the FTC. Send the actual Spam item to uce@ftc.gov. Include the full e-mail header so that your complaint can be followed up. If your complaint has to do with "remove me" or "unsubscribe" offers not working, complete and submit the FTC's complaint form at www.ftc.gov.

For more on Spam and how to avoid it, visit www.ftc.gov/spam.

Talk to Kids About Online Safety

Before your kids go online, it's a good idea to talk with them about materials they might encounter. And help them find sites that might interest them (see the list provided below). Advise them to:

- Tell you when they encounter materials they don't think they should see
- Never give out personal information
- Never fill out online forms

- Never visit adult areas on the Web

You'd be surprised how many children believe it's acceptable to give personal information about their families in order to enter an online contest. To protect your privacy, it's in your best interest to discuss acceptable online behavior with your children.

Consider a Software Filter

If you want to limit the kinds of material your child encounters while online, consider installing a software filter. The products listed below offer a variety of blocking and monitoring features.

[Cyber Patrol \(http://www.cyberpatrol.com/\)](http://www.cyberpatrol.com/)

Cyber Patrol gives you tools to help shield your children from the darker side of the Internet.

[Cyber Sentinel \(http://securitysoft.com/site/Home_Products/home_products.html\)](http://securitysoft.com/site/Home_Products/home_products.html)

Cyber Sentinel allows user to block inappropriate material (Web pages, e-mail, pictures, and word processing documents) no matter what format it is in.

[CYBERSitter \(http://www.cybersitter.com/\)](http://www.cybersitter.com/)

CYBERSitter blocks and monitors access to unsuitable and objectionable material on the Internet.

[FamilyCAM \(http://www.silverstone.net/\)](http://www.silverstone.net/)

Password-protected FamilyCAM lets parents monitor their children's computer and online whereabouts even when they can't be with them.

[I am Big Brother \(http://www.iambigbrother.com/\)](http://www.iambigbrother.com/)

This program monitors "both sides" of chat sessions, instant messages, e-mail and more while running hidden in the background.

[Net Nanny \(http://www.netnanny.com/index.html\)](http://www.netnanny.com/index.html)

This software allows parents to control all access to the computer—not only Internet resources but also offline computer use.