Cyber-cons and -scams!

Internet fraud often consists of scams that con-artists have been using for years — only now they have a new medium and new victims to exploit.

Here are some tips to help you:

- Shop on-line only with companies you know. If you don't know a company, ask for a print catalog before you decide to order electronically.
- Use a secure browser that will encrypt or scramble purchase information. If you don't have encryption software, look for software that can be downloaded from the Internet for free. Consider calling the company's 800 number, faxing your order, or paying with check.
- Never give anyone your bank account number, social security number, or other personal information that isn't absolutely needed to complete a transaction.
- Never give out your Internet password. Never. Your on-line provider will not ask for your password other than at first log-in. Change your password often and be creative!

Top scams on the Internet

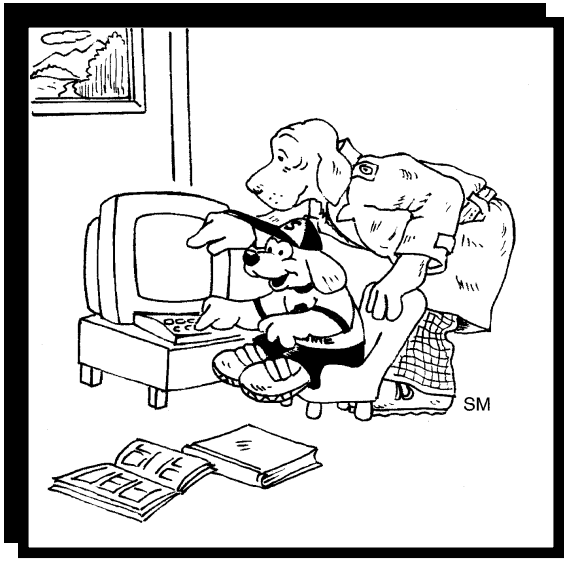
- Business opportunities or franchises that are represented as more profitable than they really are. For example, pyramid schemes offering a chance to invest in an up-and-coming company with a guaranteed high return.
- Internet-related services that are not delivered, such as a Web site design or equipment that is not delivered or is a lower quality than promised.
- Work-at-home schemes where individuals need to invest money in start-up services, but don't earn enough money to recover the initial invest-

New York State Police
www.troopers.state.ny.us

National Crime Prevention Council
2345 Crystal Drive, 5th Floor
Arlington, VA 22202
www.ncpc.org

The National Citizen's Crime Prevention Campaign, sponsored by NCPC, is substantially funded by the Bureau of Justice Assistance, Office of Justice Programs, U.S. Department of Justice.

Distribution made possible in part by a grant from ADT Security Systems, Inc.



CYBER-SAFETY

A guide for safety on-line

Distributed as a community service by the

New York State Police

The Internet has opened up a world of information and opportunity for anyone with a computer and a connection! Your safety and the safety of your children can be protected by establishing safety guidelines. You should not let your children on the information superhighway without them.

Talk to your children

- Set aside time to explore the Internet together. If your child has some computer experience, let him or her take the lead. Visit areas of the *World Wide Web* that have special sites for children.
- Explain that although a person may be alone in a room using the computer, once logged on to the Internet, he or she is no longer alone. People skilled in using the Internet can find out who you are and where you are. They can even tap into information in your computer.
- Teach children about exploitation, pornography, hate literature, excessive violence, and other issues that concern you, so they know how to respond when they see this material. The best tool a child has for screening material found on the Internet is his or her brain.

Tell your children

- Never to respond to messages that have bad words or seem scary or just weird; and to always let you know immediately if they find something scary or threatening on the Internet.
- Never to give out their name, address, telephone number, password, school name, parent's name, or any other personal information.
- Never send a picture of themselves to anyone without your permission.
- Never to agree to meet face to face with someone they've met on-line.
- Never to enter an area that charges for services without asking you first.

Control access

- Chose a commercial on-line service that offers parental control features. These features can block contact that is not clearly marked as appropriate for children — chat rooms, bulletin boards, news groups, and discussion groups — or access to the Internet entirely.

- Purchase blocking software and design your own safety system. Different packages can:
  * block sites by name,
  * search for unacceptable words and block access to sites containing those words,
  * block entire categories of material, and
  * prevent children from giving out personal information.
- Monitor your children when they're on-line and monitor the time they spend on-line.

If a child becomes uneasy or defensive when you walk into the room or when you linger, this could be a sign that he or she is up to something unusual or even forbidden.

How to protect your children when they are using someone else's computer system

- Make sure that access to the Internet at your children's school is monitored by adults.
- Make sure that your child's school has an Acceptable Use Policy (AUP). This policy should include a list of acceptable and unacceptable activities or resources, information on "netiquette", consequences for violations, and a place for you and your child to sign. (Your family can design its own AUP for the home computer.)
- Know your children's friends and their parents. If your child's friend has Internet access at home, talk to the parents about the rules they have established. Find out if the children are monitored while they are on-line.
- If your child receives threatening e-mail or pornographic material, save the offensive material and contact that user's Internet service provider and your local law enforcement agency.
- If you find sites that are inappropriate for children when you are surfing the Net, send the addresses to on-line services that offer parental control features or to sites advertising protection software to add to their list to be reviewed for inclusion or exclusion. Even if you don't subscribe to the service or own the protection software, you can help protect other children.