

Making Your Ride on the Internet Safer

You've heard the stories. Someone used his credit card for an Internet order, and his identity was stolen. Another person responded to a spam e-mail, and now she's been charged for goods she didn't receive. With so many Internet horror stories, you might wonder how you can safely take advantage of all that is good about the Internet. But, not to worry, by taking a few wise steps to protect yourself, you can have a smooth and safe ride on the Internet.

Selecting an Internet Provider

Before signing up with an Internet service provider (ISP), check its privacy policy and *spam* e-mail protection. Most ISPs today can identify incoming, unsolicited e-mail called *spam*, but do not delete them. A recently enacted law makes it illegal to send unsolicited commercial e-mail with misleading address or subject headers, or to harvest e-mail addresses without consumers' knowledge. However, unscrupulous people still violate the law.

To make it more difficult for spammers, choose a user name/ID and a password that is not your real name, but still something you can remember easily. If possible, a combination of numbers, letters, and symbols is a good idea. For example, your e-mail address could be "tough&guy%959#@aol.com".

Electronic Mail

Electronic mail, or e-mail, is the first experience many people have with the Internet. It is an easy, fast way of communicating. The major difference between e-mail and "snail mail" (mail delivered by the U.S. Postal Service) is the level of privacy one can expect.

Some of the best advice is this: Be careful what you send electronically. If you would not want something published on the front page of the newspaper, you probably should not send it via e-mail and maybe not at all. Privacy via e-mail is not guaranteed.

Use of E-Mail at Work

In a well-publicized case in 1996, an employee of a large corporation was fired when he sent a sarcastic, critical note about his supervisors to another employee using the firm's e-mail system. The fired employee filed an appeal in federal court, claiming an invasion of his privacy had occurred. However, the court upheld the corporation's right to dismiss the employee for misconduct, citing that most employment is "at will," and the employee had not been damaged by the action of his employer.

You may question your employer's right to read your e-mail in view of the Fourth Amendment, which protects against unreasonable search and seizure, and the Electronic Communications Privacy Act (ECPA), which extends federal wiretapping provisions to cover e-mail. However, courts have ruled that, as the owner of the system, the employer has the right to monitor whatever e-mail you send.

It is a good idea for employers to have a written e-mail and Internet policy and to require employees to sign it. When starting a new job, make sure you get a written copy of the policy; and, if you have questions about it, ask your supervisor. If there is no written policy, attempt to get a verbal explanation. You might have a reasonable expectation of privacy if the employer provides password protection and encryption of messages.

Surfing the Internet

Each year, millions of consumers surf the Internet to search for information and advice, to buy products and services, or simply to be entertained. A major appeal of the Internet is that it provides access to a wide variety of information without one having to get dressed or leave home. This newest communication medium, although still in relative infancy, has experienced phenomenal growth worldwide.

Like e-mail, surfing the Internet is less private than many other means of communication. While it allows the opportunity to educate oneself on a variety of topics and is often necessary for business purposes, it also enables others to gather information about you that you would not want them to know and even to commit crimes using that information.

Consumers might think that once they sign on and begin searching for information using a user name, everything they do is private. But there are a number of ways in which your Internet communication is not confidential.

Many of the Web sites you visit record information about you by using *cookies*, which are tiny files that Web sites place on visitors' hard drives so they can remember things about each visitor. While many cookies remember simple information to enhance the visitor's Web experience, many of them can identify the computer by assigning it an identification number. Marketing companies called *data miners* link these numbers with visitors' names, addresses, and other personal information that can be used to market products. They can do this without your consent or the consent of your Internet service provider.

You can prevent cookies from being stored on your hard drive by disabling them on your Internet browser program. With the *Internet Explorer*, this is done by clicking on the *Tools* menu at the top of the screen, then *Internet Options*, and then on the privacy tab. Here you can choose how you want to handle cookies.

They can be blocked completely or you can let in only certain ones that are not harmful.

When you want to buy something over the Internet, make sure your browser is in its secure mode by looking at the lower right-hand corner of the screen. A small closed padlock symbol in that corner shows it is secure. Most sites that handle financial transactions should be secure, so avoid those that are not. Also, when buying items on the Internet, it is better to use a credit card than a debit card. You will be liable for \$50 at most if someone makes fraudulent or unauthorized use of your credit card. The legal liability for debit cards, however, can be much higher, and unlimited in certain circumstances.

Never give personal information such as your Social Security number, credit card number, bank account numbers, or your address to unknown companies. Remember that you don't know who is really at the other end. If you're going to do business on the Internet, stick with companies you know.

Some Web sites ask for additional information. If you provide it, often by signing a "guest book," it can be added to a database for future use by that company or to be sold to other companies.

Your own Internet service provider can also gather information about you, keeping track of your e-mail address and which sites you visit when you surf the Internet. Much of the information that is collected about you might never be used. In fact, many companies claim they use the information only to improve their Web sites. But the information can also be used to send you unsolicited e-mail or, ultimately, it can be sold to companies that use it to create databases of personal information for marketing or other purposes.

Policies on use and sale of personal information vary from company to company. If the sale of personal information is an important issue to you, be sure to check out an ISP's privacy policy before committing to its service.

Ask your Internet service provider what kind of information it collects about you, how it is used, and whether it is ever sold. If you do not want to be included on a mailing list, be sure to let your provider know in writing.

Another danger of using the Internet is to your computer. *Viruses* and *worms* can infect your computer, possibly resulting in lost data and costly repairs. Use antivirus software and update it regularly. Also, if you have a broadband connection so that your computer is always connected to the Internet, and even if you do not, it is a good idea to install a *firewall*; that is, either software that is installed or a physical piece of additional hardware that can be connected to your computer. This provides an additional layer of protection, blocking hackers and preventing unauthorized communications between the Internet and your computer.

Ways to Increase Privacy

You don't need to disconnect your computer from the Internet in order to protect your privacy. But there are a few things you can do to make your transactions more secure and your explorations more private.

If you want to protect your anonymity when you visit a Web site, stop by this site first: <http://www.anonymizer.com>. It will assign you an anonymous identity that is revealed in place of your real identity when you visit other sites. Then click on *Free Private Surfing*.

Some Internet service providers use encryption, which is a method of scrambling electronic information to prevent it from being read by anyone other than the intended recipient. This can add a measure of security and privacy to confidential information, such as credit card numbers or personal messages.

Phishing

Phishing is the term given to Internet scammers who “phish” for Internet users’ financial

information. They send e-mail that appears to be from a legitimate financial institution, and ask for private financial records such as bank account numbers, credit card numbers, and your Social Security number. E-mails such as these are always scams. A legitimate financial institution or other company will never e-mail you for your credit card number. The only place financial institutions and reputable online retailers will take your credit card number is over a secure Web site. Never respond to e-mail asking for personal information, and never click on links in these e-mails.

Phishing scams are on the rise, with 7 out of 10 Internet users receiving such e-mails, 15% of whom have been successfully scammed into providing personal information.

Advance Fee Fraud

Another scam that arrives via e-mail is the *Advance Fee Fraud*, also known as “The Nigerian Scam” (because early e-mails of this type often came from Nigeria). These e-mails usually say you are the beneficiary of a huge sum of money, by inheritance, lottery, or from an apparently important person who claims to need your help with a bank account. The catch is that they need you to contact an “in-between” who, for a fee, will process the money for you. The end result is that you lose the money you spend on fees. The scammers will keep you going as long as they can, paying all the fees they can get you to pay. As with phishing, do not respond to these e-mails.

Spyware

Spyware is software that is secretly installed on your computer, mainly to advertise through pop-up ads or to record personal information. Besides the ads, the main annoyance with spyware is that it slows your computer and can stop programs from running, possibly even crashing your computer. Some spyware will even change your homepage on your Web

browser. If your computer displays any of these symptoms, the cause might be spyware.

Read the end-user licensing agreements before installing any software to make sure that no additional software is installed. Avoid using “free” software, most of which includes spyware as part of its cost. By using anti-spyware software, you can eliminate spyware on your computer. Like antivirus software, you will need to use it regularly to scan your hard drive.

Getting Rid of Spam E-Mail

One problem with having an e-mail account can be *spam* e-mail. *Spam* (unsolicited e-mail) often promises free products that aren’t really free, or tries to sell you junk. It is a lot like junk mail for your computer. Take action to limit and even get rid of spam entirely. Don’t respond to spam e-mail, and don’t click on the “unsubscribe” link if you do open the e-mail. This only tells the sender that your e-mail address is legitimate and to send more spam there! Simply delete the e-mail. Also, you might want to have at least two different e-mail accounts, one for family and friends and one for using on the Web, such as when you make purchases or for other times when you need to provide an e-mail address. You can get free e-mail accounts from MSN, Google, Hotmail, and other sites. Of course, the price of a “free” e-mail account usually includes putting up with all the advertisements.

Spam is now illegal according to the CAN-SPAM act, which took effect Jan. 1, 2004. To report spam to the Federal Trade Commission, forward it to spam@uce.gov.

Federal Trade Commission

The Federal Trade Commission’s (FTC) Web site is www.ftc.gov. The page to make a complaint is: <http://www.ftc.gov/spam/>. Because URLs can change at any time, you can also access this page by clicking on *File a Complaint* at the top of the FTC homepage.

The FTC’s contact information is:

Federal Trade Commission
600 Pennsylvania Ave. NW
Washington, DC 20580
1-877-FTC-HELP (1-877-382-4357)

References:

“A Tough New Anti-Spam Tool,” *Time*, September 27, 2004.

Federal Trade Commission, www.ftc.gov

“Is Someone ‘Phishing’ for Your Information,” Federal Trade Commission, March 2004.

“Privacy in Cyberspace: Rules of the Road for the Information Superhighway,” Utility Consumers’ Action Network fact sheet #18, *Privacy in Cyberspace*, March 1997.

“Protect Yourself Online,” *Consumer Reports*, September 2004. [*This article is especially helpful in selecting the best antispam, antivirus, and antispyware software, and it provides good information on phishing and other things to watch out for.*]

“Caught in a phishing trap”

http://news.com.com/Caught+in+a+phishing+trap/2100-1029_3-5453203.html, CNET News.com, November 2004.

Publication written by Robert H. Flashman, Ph.D., State Specialist in Family Resource Management; Christopher Hart, UK Undergraduate Student; and Brian Fitzpatrick, Computer Support Specialist II. Edited by Alex Lesueur, Jr., M.S.L.S., Family & Consumer Sciences Extension.

Reviewed by Kelly Razor, IS Tech Support Specialist IV; and Jamie Profitt, IT Manager, University of Kentucky College of Agriculture.

1997; revised 06/99, 01/05.

Educational programs of Kentucky Cooperative Extension serve all people regardless of race, color, age, sex, religion, disability, or national origin.

Where trade names are used, no endorsement is intended nor criticism implied of similar products not named.