

Whether conducting online transactions at your credit union or using the Internet, common sense precautions can help protect your personal information against **identity theft** and **account fraud**.

The security of your home computer is like the security of your home. The Internet is a public network, just like the streets in your neighborhood. Your ability to control who comes in depends on your security measures. Your online transactions must have security at both ends—for example, within your credit union, and within your own system.

TECHNOLOGY HELPS ENSURE SECURITY

When you use the Internet to visit your credit union, whether it's to learn about rates, review your account, pay bills, or transact other business, you are entering a secure area:

■ **PASSWORD PROTECTION**—Before using online services you develop a secret password that only **you** know. This assures that you, and only you, have access to your accounts.

■ **ENCRYPTION**—Once online with your credit union, your transactions and personal information are most likely secured by encryption software that converts the information into code readable by only you and your credit union.

■ **PRIVACY POLICIES**—Every credit union must implement a stringent privacy and security policy to protect your personal and financial information. Each member's confidential information is treated with the utmost care, meeting or exceeding federal and state mandates.

Next, consider what *you can do* to keep your end of the Internet safe.

UNDERSTANDING YOUR ROLE

No security system is 100% safe, not on your home, not on your computer. At home, you may have sturdy doors and windows, locks, and perhaps an alarm or intrusion detection system. Here are some areas of security to know about for your home computer.

■ **PASSWORDS**—Your password is the key that opens your home computer. You wouldn't use a passkey on your front door. Similarly, don't use a password that is easy for others to guess such as birth dates, Social Security numbers, child or pet names. Instead, use a password that contains a variety of letters, numbers, and symbols and change it regularly.

■ **ANTI-VIRUS SOFTWARE**—Anti-virus software should be installed on all Internet-connected computers. Many computers come with this software, but you have to make sure it's turned on. Your anti-virus software is like your annual flu shot. Your first installation protects you for a while, but because new viruses are emerging daily, it is essential to update your anti-virus software regularly.

■ **FIREWALLS**—A firewall is the protective shell between your computer and the outside world. It reduces threats to your home computer from the Internet by filtering out potentially dangerous data and preventing unauthorized access to your computer. Updates to firewalls are called patches. Your software company may notify you by e-mail when it releases a new patch, but you should check your software company's Web site regularly to make sure that you don't miss one.

■ **ENCRYPTION**—Encryption is the scrambling of your private information to prevent unauthorized data capturing. If you communicate through a secure Web page like your credit union's, the information you transmit is almost certainly encrypted. However, email is frequently unencrypted, even if you access it from a secured web page, so be wary of sending sensitive information such as account numbers through e-mail.

■ **OPERATING SYSTEMS**—You should regularly check on whether new security updates are available for your computer operating system (i.e., Windows, MacOS).

■ **DISCONNECT**—Turn off your computer or disconnect from the Internet when you are not using it. An intruder cannot attack your computer if it is turned off or otherwise completely disconnected from the Internet.

■ **BACK UP YOUR DATA**—Even with all these security measures in place, the information on your computer is still vulnerable. Protect yourself from loss of critical data by backing up your files.

WATCH FOR THESE THREATS

■ **UNKNOWN E-MAILS, ATTACHMENTS, AND PROGRAMS**—Before opening any e-mail or attachments, make sure you know where they came from. If you must open an e-mail or attachment before you can verify the source, following these steps will reduce the chance that any malicious code contained in the attachment might spread to your computer:

- 1 make sure your virus definitions are up to date
- 2 save the file to your hard disk
- 3 scan the file using your anti-virus software
- 4 open the file

For additional protection, disconnect your computer's network connection before opening the file.

■ **FRAUDULENT WEB SITES (PHISHING)**—Copycat Web sites deliberately use a name and Web address that is deceptively close to the Web address of a genuine business. The trick is to lure you into clicking onto their Web site and giving them personal information, such as your account number and password. With this information, the operator of this Web site may put charges on your credit card, steal from your

accounts, and even steal your identity. Always make sure that you have typed the correct Web site address, and that you are familiar with the home page, before conducting any business or disclosing any personal information.

You can visit your credit union's Web site at any time, day or night—that's convenience! Your credit union is doing its part to make the journey safe and with some simple, common sense precautions, you can do your part!



Presented by the National Association of Federal Credit Unions, an independent trade association representing federally chartered credit unions nationwide.

© 2005 FINANCIAL EDUCATION CORPORATION

INTERNET SAFETY TIPS

Online safety and security is a team effort. Here is what your credit union is doing...and what you must do.