Guarding Against

E-MAIL & INTERNET FRAUD

What credit union members should know to counter

- **Phishing**
- **Pharming**
- **Spyware**
- **Online fraud**

On-Line Fraud Is Growing

E-Mail and Internet Fraud take advantage of the Internet's unique ability to send e-mail messages worldwide in seconds or post Web site information that is accessible from anywhere. E-mail and internet fraudsters carry out their scams more invisibly than ever before, making identity theft from online scams one of the fastest growing crimes today.

Credit union members should be especially vigilant to some of the more prevalent frauds at work in cyberspace:

PHISHING Fraudulent e-mails, appearing to be from a trusted source such as your credit union or a government agency, direct you to a Web site asking you to "verify" personal information. Once scammers have your information, they have the tools to commit account fraud *using your name.*

✔ What You Can Do:

- If you receive an e-mail that tells you to confirm certain information, **do not** click on the e-mail link. Instead, use a phone number or Web site address you know to be legitimate.
- Before submitting any financial information through a Web site, look for the "lock" icon on the browser status bar, or look for "https" in the Web address.
- Report suspicious activity (see resources section of this brochure).

Remember: Your credit union will never send you an e-mail asking you to verify personal information!

PHARMING Similar to phishing, pharming seeks to obtain personal information by secretly directing you to a copycat Web site where your information is stolen, usually with a legitimate-looking form.

✔ What You Can Do:

- Be wary of unsolicited or unexpected e-mails from all sources.
- If an unsolicited e-mail arrives, treat it as you would a phishing source (see above).

MALWARE Short for malicious software, and also known as "spyware," it is often included in spam e-mails. It then can take control of your computer and forward personal data to fraudsters.

✔ What You Can Do:

Install and update regularly your:

- Anti-virus software
- Anti-malware programs
- Firewalls on your computer
- Operating system patches and updates

GENERAL TIPS AGAINST CYBER-FRAUD

- **Don't Judge by Initial Appearances.** The availability of software that allows anyone to set up a professional-looking Web site means that criminals can make their Web sites look as impressive as those of legitimate businesses.

UNDERSTANDING MULTI-FACTOR AUTHENTICATION

New ways to verify identities should make internet transactions safer than ever

Your credit union wants to be sure that the level of authentication (i.e., the way you identify yourself and the security measures you employ) used in a particular transaction is appropriate to the level of risk in that application. As a result, you might begin to experience some changes in how you identify yourself and gain access to your accounts over the Internet. For example, you might need to utilize some form of *multi-factor authentication.*

Today's authentication methods involve one or more basic "factors":

- Something the user ***knows*** (e.g., password, PIN)
- Something the user ***has*** (e.g., ATM card, smart card)
- Something the user ***is*** (e.g., biometric characteristic, such as a fingerprint)

Single-factor authentication uses *one* of these methods; ***multi-factor*** authentication uses *more than one*. When you log on with a password, you are using single-factor authentication; when you use your ATM, you are using multi-factor authentication: Factor number one is something you *have*, your ATM card; factor number two is something you *know*, your PIN.

In addition to any new authentication measures, you can be assured that your credit union is working to make your online transactions safer and more convenient than ever before using

- **Password Protection**
- **Encryption Technology**
- **Privacy Practices and Policies**

- **Be Careful Giving Personal Data Online.** If you receive e-mails from someone you don't know asking for personal data—don't send the data without knowing who's asking.

- **Be Wary of E-mails Concealing Their True Identity.** If someone sends you an e-mail using a mail header that has no useful identifying data it could mean that the person is hiding something.

- **Fortify Your System.** Here are some basic safety tips you can implement immediately:
  - ***Password***—Experts advise a combination of letters and numbers.
  - ***Virus Protection***—Your computer's anti-virus software needs to be up-to-date to guard against new strains.
  - ***Firewalls***—This protective wall between the outside world and your computer helps prevent unauthorized access. Check regularly with your software company to be sure you have the latest updates.
  - ***Spyware***—Anti-spyware programs are readily available. Every computer connected to the Internet should have the software installed…and updated regularly.

RESOURCES

- **Internet Fraud Complaint Center (IFCC)**
  www.ifccfbi.gov
- **Consumer Fraud (DOJ/Homepage)**
  www.usdoj.gov
- **Federal Trade Commission (FTC) Consumer Response Center**
  www.ftc.gov
- **FirstGov (Your First Click to the U.S. Government)**
  www.firstgov.gov
- **Consumer.gov**
  www.consumer.gov
- **Social Security Administration**
  Report Fraud: 800-269-0271
- **Identity Theft Resource Center**
  www.idtheftcenter.org
  858-693-7935

Drop by your credit union to learn more about how they are making online transactions safe and secure!