

Understanding the New ELECTRONIC AUTHENTICATION

Multi-factor Authentication and Layered Security is helping to assure safe Internet Transactions for our Credit Union and Members

When you visit our credit union online in the coming months, you will notice some changes. These changes have to do with how you identify yourself and gain access to your accounts over the internet, and are designed to make you safer than ever before from account hijacking and identity theft. These changes are based on the realization that internet fraudsters have become increasingly sophisticated, making single-factor authentication (a simple password, for example) inadequate for some of your online financial transactions.

Understanding the Factors

Today's authentication methods used to confirm that it is you, and not someone who has stolen your identity, 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*, and thus is considered to be a more reliable and stronger fraud deterrent. When you use your credit union 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.

Risk Assessment Results

Our credit union's goal is to ensure that the level of authentication used in a particular transaction is appropriate to the level of risk in that application. Accordingly, our credit union has concluded a comprehensive risk assessment of

its current methods following stringent Federal regulatory guidelines and will be implementing the appropriate authentication measures to keep your online transactions safe and secure. In addition to single and multi-factor authentication, our credit union may also rely on several layers or controls to assure your Internet safety. These layers might include:

- Additional controls, such as call-back (voice) verification, e-mail approval, or cell phone based identification.
- Employing member verification procedures, especially when opening accounts online.
- Analyzing certain transactions to identify suspicious patterns
- Establishing dollar limits that require manual intervention to exceed a preset limit.

Importantly, the methods used will be those needed to assure your safety and security when conducting online financial business. It's our credit union's top priority!

Member Awareness: The First Line of Defense

Of course, understanding the risks and knowing how fraudsters might trick you is a critical step in protecting yourself online. Here are some threats to watch for:

Phishing: lures you to a fake website (one that looks like a trusted financial institution) and tricks you into providing personal information, such as account numbers and passwords.

Pharming: similar to phishing, pharming seeks to obtain personal information by directing you to a copycat website where your information is stolen, usually from a legitimate-looking form.

Malware: Short for malicious software, often included in spam e-mails, this can take control of your computer without your knowledge and send to fraudsters your personal information such as Ids, passwords, account numbers and PINs.

You can make your computer safer by installing and updating regularly your: Anti-virus software, Anti-malware programs, Firewalls, Operating System patches and updates

RESOURCES

The following websites can get you started learning about your online security options. These are provided for information purposes; no endorsement of any product or service is intended.

Multi-Factor Authentication

Federal Financial Institutions Examination Council
www.ffiec.gov/press/pr101205.htm

Anti-Virus & Firewall

Norton Anti-Virus
www.symantec.com

ZoneAlarm
www.zonelabs.com

Spyware AdAware
www.adaware.com

Windows Defender Microsoft AntiSpyware
www.microsoft.com

Stop by the credit union to learn more about these important ways that your online experience is being made safer and more convenient than ever.

Guarding Yourself Against Internet And Email Fraud

To Counter PHISHING, PHARMING, SPYWARE and ONLINE FRAUD

On-Line Fraud Is Growing

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). Remember: We 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.

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.

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.

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 is 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 antivirus 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.ifcctbi.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