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 forward 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 on your computer
- 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
McAfee Anti-Virus
www.mcafee.com

Norton Anti-Virus
www.symantic.com

ZoneAlarm
www.zonelabs.com

Spyware
AdAware
www.adaware.com

Microsoft AntiSpyware
www.microsoft.com

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

NOTE: *Quotations are from Federal Financial Institutions Examination Council's "Authentication in an Internet Banking Environment."

Understanding the New

ELECTRONIC AUTHENTICATION

Multi-factor authentication **and** ***layered security*** **are helping assure safe Internet transactions for** ***credit unions*** **and their** ***members.***

Assuring Your Online Security

When you visit your credit union online in the coming months, there's a good chance you'll 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.

"Financial institutions offering internet-based products and services… should use effective methods to authenticate the identity of members…"

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":

"Account fraud and identity theft are frequently the result of single-factor authentication exploitation"

- 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

Your 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, your 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.

"An effective authentication system is necessary…to safeguard member information, prevent money laundering and terrorist financing, reduce fraud, inhibit identity theft and promote the legal enforceability of electronic agreements and transactions."

In addition to single and multi-factor authentication, your credit union may also rely on several ***layers of control*** 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.

"Financial institutions should rely on multiple layers of control to prevent fraud and safeguard member information."

- 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 your 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, for example) and tricks you into providing personal information, such as account numbers and passwords.