

Security Alert for CU Online Users

Customers of some local financial institutions have recently begun receiving fraudulent e-mails regarding their accounts. This process known as “phishing” is used as an attempt to gain access to your personal information. The technique involves sending e-mails that are designed to appear that they are coming from a legitimate financial institution and will normally request that you login to a website to update your account or password information.

The important thing to know about “Phishing” is that it’s a random process. If you receive a message, it doesn’t mean that the perpetrator has any information about you. The message was sent to thousands of accounts in the hope that someone will fall for the scam.

The rise of “phishing” and other Internet fraudulent activity does not mean that CU Online or other ecommerce activities are unsafe, only that it is important to be aware of where you are entering your personal information.

While there have been no reported incidents concerning FORUM Credit Union, we want to take this opportunity to pass along these important safety reminders.

✓ FORUM Credit Union will never send you an Internet e-mail asking for your account number or password. If you receive such a message, please forward it to us at fraud@forumcu.com or contact Member Services at 1-800-382-5414.

✓ Pick a secure password and never reveal your CU Online password to anyone. Passwords should contain a combination of letter and numbers, and should not include any part of you account number or name. It is also suggested that you avoid other easy to guess words such as names of your children or pets..

✓ Change your password on a regular basis.

✓ When accessing CU Online, always look for the lock at the bottom of the page indicating that you are accessing a secure page.

✓ Do not send critical account information through regular Internet e-mail. Internet e-mail is not secure. The only secure way to send a message is through the ‘Your Mail’ portion of CU Online.

✓ Always access CU Online by clicking on the link from the main FORUM Credit Union web page. If you prefer, you may create a bookmark from this link for easier future access.

✓ If you receive an unsolicited message providing a new link, do not use it. Recent Internet vulnerabilities have made it easy to create fake pages that can be used inappropriately to gather data, and the pages are often spread via e-mail.

✓ Ensure that your PC has anti-virus software and that it is updated regularly. Old software that is out of date is not effective at stopping newly created viruses.

✓ Regularly download and install manufacturers’ security patches for your operating system and web browser.

For more information on the recent “phishing” vulnerability findings, please visit the Federal Trade Commission at <http://www.ftc.gov/bcp/online/pubs/alerts/phishingalrt.htm>.

For a list of general Internet safety articles, please visit <http://www.ftc.gov/bcp/menu-internet.htm>.

If you feel that your have been a victim of Internet fraud related to your FORUM Credit Union

account, please contact Member Services at 1-800-382-5414 or send an e-mail to fraud@forumcu.com.

Other organizations to contact:

Credit Bureau Fraud Hotlines

Equifax: 1-800-526-2895

Experian: 1-888-397-3742

TransUnions: 1-800-680-7289

Social Security Administration: 1-800-269-0271

Federal Trade Commission Identity Theft Hotline: 1-877-ID-THEFT

