

Community Financial has recently experienced an increase in phishing attempts, be aware!

Online fraud and identity theft have been hot topics over the past several years. Now phishing has seemingly become the fraud tool of choice by computer con artists. Community Financial has seen an increased volume of phishing attempts to members and non-members. Financial institutions all over the country have come under attack in recent months.

To avoid becoming a victim of a phishing attempt, here is important information you should know:

What is phishing?

Phishing is a type of deception designed to steal your valuable personal data, such as account numbers, passwords, credit/debit card numbers and details, or other information. Con artists send millions of fraudulent e-mail messages that appear to come from websites you trust, like your financial institution or credit card company, requesting that you provide personal information to maintain your account. As scam artists become more sophisticated, they often include official-looking logos from real organizations and other identifying information taken directly from legitimate Web sites. To make these phishing e-mail messages look even more legitimate, the scam artists may place a link in them that appears to go to the legitimate website, but it actually takes you to a phony scam site or possibly a pop-up window that looks exactly like the official site. Any information given could be used in fraudulent transactions attempts.

How do con artists get my e-mail address?

Con artists use other computers connected to the Internet to do the dirty work (stealing email contacts), so it's hard to trace the origin of the phish.

Most Important:

As a Community Financial member, **the main thing to remember is that Community Financial will never solicit personal information such as account numbers, credit or debit account numbers, SSN, PINs, or passwords via mail, phone or e-mail. So if you receive such a solicitation from "Community Financial," or any other institution, NEVER provide the information requested. Responding to a Phishing request could result in fraudulent transactions and financial losses to you that are not eligible for reimbursement. Instead, contact the institution to report the solicitation.**

What can I do to verify the validity and authenticity of a website or phone number?

If you receive a solicitation to click on a link in an e-mail or call a phone number to verify account information, instead, call the institution's established contact information to verify the request. Community Financial's official phone numbers are (734) 453-1200 or (877) 937-2328. Any solicitation you receive to call a different number and confirm secure information is fraudulent.

Another thing to remember about these phishing e-mail attacks is that the con artist has only stolen your e-mail addresses. **Rest assured, they ARE NOT getting inside firewalls and accessing actual account information.** If they had that ability, they would not be trying to trick people into giving them information.

Make sure the address on your browser's address bar is the legitimate address of the site you intended to visit. For example, the base address you will see on your browser's address bar if you visit Community Financial's website is <http://www.cfcu.org>. If you continue on to our online banking service, the base address is **<https://www.cfcu.org>**. Since these are legitimate, registered addresses, fraudsters cannot use them to trick you into thinking it's our authentic site. Therefore, always make sure the address you see on your address bar is the registered address. If the address is different, it's fraudulent.

What security measures do Community Financial have in place?

1. We monitor our network 24/7 to ensure the safety and security of our members' information. We also partner with experienced network consultants who advise us on best practices to prevent intrusion from potential hackers.
2. We contract with an Internet security company that works with Community Financial to block access to sites that are deemed suspicious.
3. We have security-auditing firms who assist us in identifying potential vulnerabilities. If any vulnerability is found, improvements are implemented to eliminate it.
4. We have updated our website to include anti-phishing technologies that add an extra layer of protection. For certain browsers, an extended validation certificate appears on our site pages to identify them as authentic Community Financial web pages. If a con artist reproduces the pages these certificates will not appear, letting you know you're not on an authorized Community Financial page.

Again, please remember: **do not provide sensitive information if solicited.** If you have any questions or have experienced a phishing attempt that impersonated Community Financial, please call (734) 453-1200 or (877) 937-2328, toll free, as soon as possible.