

# Protect Yourself from Phishing, Vishing, and Other Fraudulent Scams

Copper Basin Federal Credit Union (CBFCU) members and non-members may be targeted by fraudulent emails. We want our members and all financial consumers in the area to be informed, alert and protect themselves from these **Phishing** scams.

These Phishing e-mails are not from CBFCU and do NOT affect the credit union's actual data system and at no time has that information ever been compromised. These scams are aimed squarely at consumers in an effort to trick them into providing their own personal information for use in criminal or fraudulent activities.

Consumers in the area may also receive an automated telephone message telling them that the Copper Basin Federal Credit Union system was undergoing security updates and changes and asking them to update their personal information. Other variations of these **Vishing** calls may be used, but again these are scams aimed at consumers in an effort to trick them into providing their own personal information for use in criminal or fraudulent activities.

The criminals behind these scams simply blast a large number of emails (or automated calls) out to the public hoping to hit some people who are actually our members. Of course they are hoping someone will actually respond with their personal account information.

Education, information, and diligence on the part of consumers are among the best ways to protect yourself against such fraud activities. CBFCU and other financial institutions typically provide links and other beneficial information about such scams on their websites. In an effort to minimize or drastically reduce the impact of such scams, CBFCU is providing consumers with the following information and resources:

**Phishing Scam:** Fraudulent e-mails containing the targeted institutions logo and name aimed at consumers, trying to trick them into giving out personal information such as credit/debit/ATM card numbers, PINs, expiration dates and other sensitive or personal financial information.

**Vishing Scam:** Similar to Phishing, except by phone...either in person or by an automated phone system. These criminals will claim to be from the financial institution whose customers are being targeted. They will request the same type of personal and account information.

## **Always Remember:**

- NEVER give out personal information if you have NOT initiated the transaction or call.
- No legitimate financial institution will ever e-mail or call to verify personal and/or account information because if they do business with you they already possess it.
- Always verify e-mail/website addresses and phone numbers with a legitimate source such as your account statement or the phone book...do not rely on information contained in an e-mail or a phone message.
- Consumers are advised to be highly suspicious when receiving messages directing them to call and provide credit card or bank numbers. Rather than provide any information, the consumer is advised to contact their financial institution or credit card company directly to verify the validity of the message.
- If a credit/debit card company actually calls to notify you of suspicious charges, they will not ask for your personal information. Instead they will verify that they have reached the cardholder and ask for them by name. Then they may ask the cardholder to verify the last 4-digits of their Social Security Number (Note: They will NOT ask for the entire Social, Account, Expiration, or PIN). They will then verify if you made that particular charge or not. If anything sounds suspicious, hang up and call your financial institution directly.

- If you have fallen victim to such a scam and given out your personal account information contact your financial institution immediately to protect your accounts, block your cards, and take other measures as necessary.

For more information on Phishing, Vishing, and other fraudulent scams:

- Federal Trade Commission -- [www.ftc.gov/bcp/edu/microsites/idtheft/index.htm](http://www.ftc.gov/bcp/edu/microsites/idtheft/index.htm)
- US Department of Justice -- [www.usdoj.gov/whatwedo/whatwedo\\_if.html](http://www.usdoj.gov/whatwedo/whatwedo_if.html)
- Internet Crime Complaint Center -- [www.ic3.gov](http://www.ic3.gov)
- Securities and Exchange Commission -- [www.sec.gov/investor/pubs/phishing.htm](http://www.sec.gov/investor/pubs/phishing.htm)

## Fight Fraud and Identity Theft

Don't become a victim. Know what to be watching for.

- [Will the Credit Union ever send an e-mail to have me update my account information?](#)
- [What is Phishing?](#)
- [What is Pharming?](#)
- [Who to contact if you have been attacked by an identity thief.](#)
- [Keeping your information safe.](#)

- **Will the Credit Union ever send an e-mail to have me update my account information?**

No.

Always remember that CBFCU will NEVER ask you to click on an e-mail link to share sensitive financial information. Please notify us whenever you receive a suspicious e-mail or have any other form of unsolicited contact from individuals seeking personal information about your CBFCU accounts.

To verify that you are at CBFCU's official Virtual Branch E-Services site, always remember to look for your PASSMARK (*the picture and phrase that you selected*). If you don't see your PASSMARK, then don't enter your PIN/Password or any other personal information.

- **What is Phishing?**

According to [webopedia.com](http://webopedia.com):

(fish'ing) **(n.)** The act of sending an e-mail to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft. The e-mail directs the user to visit a web site where they are asked to update personal information, such as passwords and credit card, social security, and bank account numbers, that the legitimate organization already has. The Web site, however, is bogus and set up only to steal the user's information. For example, 2003 saw the proliferation of a phishing scam in which users received e-mails supposedly from eBay claiming that the user's account was about to be suspended unless he clicked on the provided link and updated the credit card information that the genuine eBay already had. Because it is relatively simple to make a Web site look like a legitimate organizations site by mimicking the HTML code, the scam counted on people being tricked into thinking they were actually being contacted by eBay and were subsequently going

to eBay's site to update their account information. By spamming large groups of people, the "phisher" counted on the e-mail being read by a percentage of people who actually had listed credit card numbers with eBay legitimately.

Phishing, also referred to as *brand spoofing* or *carding*, is a variation on "fishing," the idea being that bait is thrown out with the hopes that while most will ignore the bait, some will be tempted into biting.

Other forms: phish (v.)

- **What is Pharming?**

According to [webopedia.com](http://webopedia.com):

Similar in nature to e-mail phishing, pharming seeks to obtain personal or private (usually financial related) information through domain spoofing. Rather than being spammed with malicious and mischievous e-mail requests for you to visit spoof Web sites which appear legitimate, pharming 'poisons' a DNS server by infusing false information into the DNS server, resulting in a user's request being redirected elsewhere. Your browser, however will show you are at the correct Web site, which makes pharming a bit more serious and more difficult to detect. Phishing attempts to scam people one at a time with an e-mail while pharming allows the scammers to target large groups of people at one time through domain spoofing.

- **Who to contact if you have been attacked by an identity thief.**

If you are a member of CBFCU and responded to a message by sharing personal financial information, please contact us immediately by phone (the number is listed below for your convenience). We will give you instructions for changing your password and taking other steps to protect your accounts. Our main number is 423-496-3812.

- **Keeping your information safe.**

Always remember that CBFCU will NEVER ask you to click on an e-mail link to share sensitive financial information. Please notify us whenever you receive a suspicious e-mail or have any other form of unsolicited contact from individuals seeking personal information about your CBFCU accounts.

To verify that you are at CBFCU's official Virtual Branch E-Services site, always remember to look for your PASSMARK (*the picture and phrase that you selected*). If you don't see your PASSMARK, then don't enter your PIN/Password or any other personal information.