

Phishing Alert: Take Steps to Protect Yourself From Online Fraud

– *"We suspect an unauthorized transaction on your account. To ensure that your account is not compromised, please click the link below and confirm your identity."*

– *"During our regular verification of accounts, we could not verify your account information. Please click here to update and verify your information."*

If you receive an e-mail message similar to these, don't bite. They are examples of a scam called "phishing" and the perpetrators of this crime want one thing: your personal information. That may include your Social Security number, your account or credit card numbers, your password or login information. Giving this information can result in identity theft, which can wreak havoc with your credit report and your ability to get credit and loans in the future.

Clinton County Federal Credit Union wants you to be informed. Know how to protect yourself from this devastating financial crime:

*** Never respond to or click on e-mail requests for personal information, particularly if you are asked to verify your account information. Phishers copy logos from financial institution Web sites and use look-alike headers to trick victims into handing over personal information.**

*** Be suspicious of any e-mail that's not personalized with your name; valid messages from Clinton County Federal Credit Union are personalized. We would never ask you for personal information in this manner.**

*** Be suspicious of urgent e-mail requests claiming to be from Clinton County Federal Credit Union or from any other financial institution. Phishers typically include upsetting or exciting--but false--statements to get you to react quickly.**

*** Never click on links within an e-mail message to get to a Web page. Instead, call the company on the phone, or log onto the Web site directly by typing the company's Web address in your browser.**

*** If you access your accounts online, regularly log into those accounts. Don't ignore your accounts for as long as a month before you check them.**

*** Regularly check your credit union and credit card statements to make sure all transactions are legitimate. If anything looks suspicious, contact us or the affected issuer immediately.**

*** Use antivirus software and a firewall, and keep them up to date. Download updated security patches. For example, if you use Microsoft Internet Explorer, go to microsoft.com/security/ to download a special patch relating to certain phishing schemes.**

If you think you've been a victim of a phishing attack, notify us immediately. File a complaint at www.ftccomplaintassistant.gov/, and then visit the FTC's identity theft Web site at ftc.gov/bcp/edu/microsites/idtheft/. Victims of phishing also can become victims of identity theft, so take steps to minimize your risk. Check your credit reports regularly to see if a thief has opened fraudulent accounts in your name. Visit www.annualcreditreport.com for details on ordering a free annual credit report from each of the three major credit-reporting agencies—Equifax, Experian, and TransUnion.

If you have any questions—about phishing, or about any suspicious financial e-mail you receive—please call us at 989.224.9511. Clinton County Federal Credit Union is dedicated to help you stay safe and protect your financial resources.