



Phishing

“Phishing” is an email scam that attempts to trick consumers into revealing personal information, such as their credit or debit account numbers, checking account information, Social Security numbers, or banking account passwords through fake Web sites or in a reply email.

Phishing scams are among the fastest growing forms of fraud on the Internet. According to the Anti-Phishing Working Group, phishing scams grew by 52 percent from December 2003 to January 2004. Find out more about phishing below.

How to spot a phishing email:

Phishing emails, and the Web sites they link to, typically use familiar logos and familiar graphics to deceive consumers into thinking the sender or Web site owner is a government agency or a company they know. Sometimes the phisher urges intended victims to “confirm” account information that has been “stolen” or “lost.” Other times the phisher entices victims to reveal personal information by telling them they have won a special prize or earned an exciting reward.

Look for these red flags in the email:

- Asks you to provide personal information such as your credit union account number, an account password, credit card number, PIN number, mother’s maiden name, or Social Security number. The CAHP Credit Union will never ask you for this information by email.
- Does not address you by your name.
- No confirmation of the company that does business with you, such as referencing a partial account number.
- Warns that your account will be shut down unless you reconfirm your financial information.
- Warns that you’ve been a victim of fraud.
- Spelling or grammatical errors.



Take these steps to minimize your phishing risk:

View any email request for financial information or other personal data with suspicion.

Do not reply to the email and do not respond by clicking on a link within the email message.

Contact the actual business that allegedly sent the email to verify if it is genuine. Call a phone number or visit a Web site that you know to be legitimate, such as those provided on your monthly statements.

Do NOT send personal information (e.g., credit or debit card number, Social Security number, or PIN) in response to an email request from anyone or any entity.

Be cautious. Check your monthly statements to verify all transactions.

Forward any emails claiming to be from Visa or the CAHP Credit Union asking you to provide your personal account information to phishing@visa.com. You can also forward any suspicious email to the Better Business Bureau at nophishing@cbbb.bbb.org, and immediately call the Credit Union.