

# E-MAIL FRAUD



## Guarding against E-mail and internet Fraud

**Phishing:** Fraudulent e-mails, appearing to be from trusted source, direct you to a Web site asking you to “verify” personal information.

**Pharming:** Attack aiming to redirect a website’s traffic to another website, usually with a legitimate-looking form.

**Malware:** Short for malicious software, and also known as “spyware”, it is often included in spam e-mails. It then can take control of your computer and forward personal data to fraudsters.

### What you can do:

If you receive an e-mail that tells you to confirm information, do not click on the e-mail link. Instead, use a phone number or Web site address you know to be legitimate.

Before submitting any financial information through a Web site, look for the “lock” icon on the browser status bar, or look for “https” in the Web address.

Be wary of unsolicited or unexpected e-mails from all sources.

Don't judge by initial appearances. The availability of software that allows anyone to set up a professional-looking Web site means that criminals can make their Web sites look legitimate.

Install and update regularly your:

- Anti-virus software
- Anti-malware and Anti-spyware programs
- Firewalls on your computer
- Operating system patches and updates
- Implement and operating system password

**California Bear Credit Union accounts.**  
Designed with your security in mind.

Online banking, Telebear,  
Online Bill Payment and E-Statements.

Go to our website [www.calbearcu.org](http://www.calbearcu.org)  
or call 1.800.954.2327

**Apply Today!**



**California Bear**  
CREDIT UNION  
YOU CAN BANK ON THE BEAR™