

# SCAM ALERT #2

## Scam artists go "phishing" for financial information

**Phishing** is a method scammers use to obtain confidential information via the Internet ... and the practice is growing. This new favorite sport of scammers comes in a convincing disguise, making it easy for recipients of phishing e-mails to be fooled.

### **HOW IT WORKS:**

The scammer creates a website that very closely matches the look and content of a given financial institution's or retailer's site. Next, e-mails are sent with subject lines that include the name of the financial institution. The e-mail tells recipients that there is a chance their account has been compromised and directs them to click a link in the e-mail. The link, of course, brings the recipient to the bogus financial website and instructions to key in personal, financial information to "verify" the potentially compromised account.

Even relatively savvy Internet users can be caught by phishers because the scammers' web pages show a fake browser bar that contains the real web address of the financial organization being "impersonated."

### **THE PROBLEM:**

Any information keyed into these fake pages is actually being fed to the scam artist, who then can use the confidential information to conduct transactions using the ill-gotten personal data.

### **AVOID BEING PHISHED:**

**Be skeptical** - If you rarely use the account in question or anything about the e-mail or website looks unusual, call your financial institution (or online retailer) to verify that the e-mail is legitimate. SEFCU never requests confidential information via unsecured e-mail.

**Check for the secure site "padlock"** - Secure sites normally show a closed padlock icon at the bottom of the screen to indicate you are entering confidential information in a secure environment. Without it, chances are your data isn't secure.

**Check the properties** - Right click on any web page and you should see a list of properties, including the web address of the site. If you right click and do not get a list of properties or the web address does not match your financial institution's, don't enter any information.

SEFCU is committed to helping members protect themselves against fraud. This is the first in a series of SCAM ALERTS to educate members about deceptive activities that could harm members' financial security. While we cannot advise members of every scam, we hope the series will advance awareness of privacy and security issues.