

Don't be the catch of the day

- Monitor your accounts frequently.
- Review statements closely and report any suspicious activity immediately to the source of the statement. If you've been phished, alert the company that's been spoofed.
- If you're quick enough, you might be able to change your password or account number in time to stop unauthorized transactions.

Free Credit Report

Check your credit report for errors by ordering a free credit report from each of the major credit bureaus once each year. Request a copy at annualcreditreport.com, 877-321-8273.

SAMPLE



Center for Personal Finance
cuna.org

To order: 800-356-8010, ext. 4157

© 2008 Credit Union National Association Inc.,
the trade association for credit unions in the U.S.

Phishing: Stay Off the Hook



Phishers send fraudulent e-mails containing authentic-looking logos and familiar graphics, but lead to fake Web sites. You're asked to divulge account information or other personal data such as usernames, passwords, and Social Security numbers (SSNs).

Even the most tech-savvy consumers can become victims—so beware.

Be a smart Internet user

▶ Install a firewall. This is the primary block between you and other computers on the network.

▶ Use antivirus and antispyware protection and update it routinely. This software spots infected e-mail attachments and other virus carriers, and spyware or adware before they have a chance to harm—or hijack—your computer. Visit download.com to check ratings of spyware removal programs.

▶ Download security upgrades from your operating system vendor. Set your computer to do so automatically.

▶ Create strong passwords. Combine numbers, symbols, and letters—in upper and lower case—of at least eight characters. Avoid personal information, login names, or adjacent keyboard symbols.

▶ Change passwords often—every three to six months. If your information is compromised, your passwords should be out-of-date by the time crooks try to sell the data.

▶ Be on your guard with unsolicited e-mail and ignore requests for personal financial infor-

mation—never send sensitive personal information to anyone using e-mail. If you get a message asking you to verify credit union account information, it did not come from your credit union, where this information already is on file. Call someone at your credit union to report the attempt.

▶ Confirm the identity of the e-mail's author before clicking on attachments—viruses often are activated this way; and, instead of clicking on links within e-mail, open a new browser window and type the URL (uniform resource locator) in the address bar.

▶ Use a phishing filter or popup blocker while surfing the Web.

▶ Make sure the Web sites you shop on show a padlock in the frame of your browser window. The padlock signifies use of SSL (secure sockets layer) technology. URLs that require a safe connection start with https: or s-http: ▶

As many as 60% to 70% of PC users don't have current security software.

