using passwords with a combination of letters (upper and lowercase), numbers, and symbols.

- *Request a free copy of your credit report from the three major credit-reporting agencies*—Experian (*experian.com*, 888-397-3742); Equifax (*equifax.com*, 800-685-1111); and TransUnion (*transunion.com*, 800-888-4213). The Fair and Accurate Credit Transactions Act (FACT Act) requires each major credit bureau to provide one free credit report annually to consumers who request a copy (*annualcreditreport.com*, 877-322-8228).

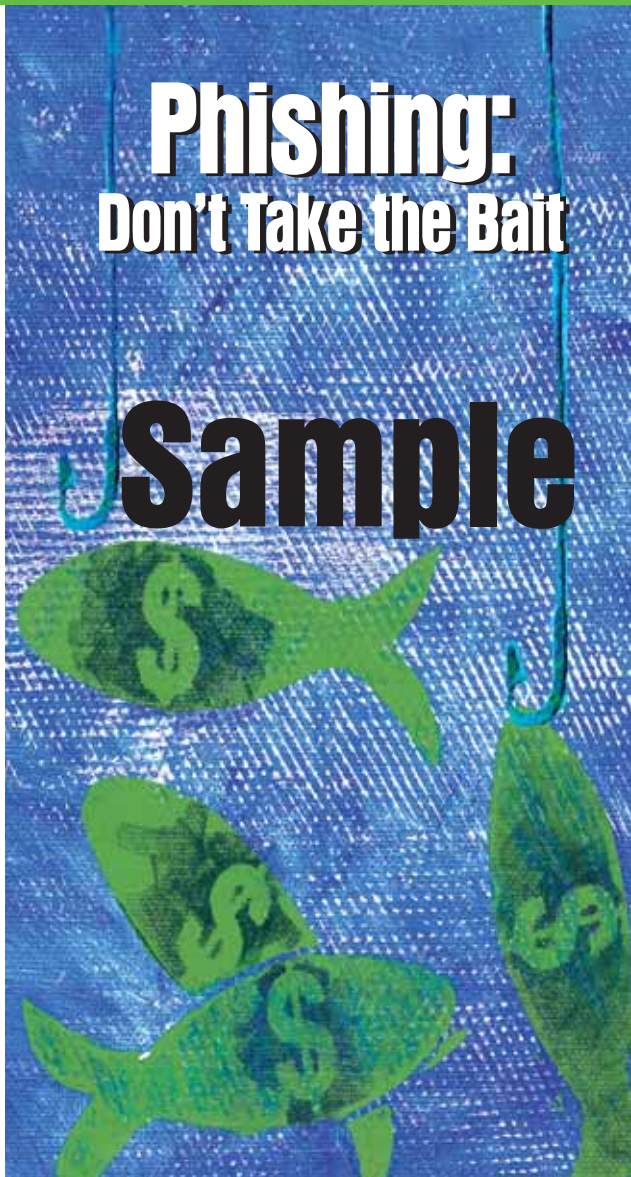
If you've mistakenly taken the bait, call the company that's been spoofed right away. If you're [illegible] your password or other personal information, [illegible].

CUNA
Credit Union National Association
Personal Finance

AMERICA'S CREDIT UNIONS™

cuna.org
To order: 800-356-8010, ext. 4157
Stock No. 27032-PRO

Phishing: Don't Take the Bait

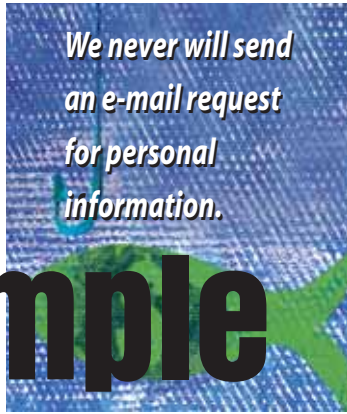


Phishers use spam—unwanted e-mail—to lure people into fake Web sites to obtain personal information and commit identity theft. Victims receive fraudulent e-mails containing authentic-looking logos and familiar graphics. They often will lead to a "spoofed," or fake site that looks authentic. You're asked to divulge account information or other personal data such as usernames, passwords, and Social Security numbers.

Your credit union never will send you an e-mail—or call you by phone—asking for personal data. We already have this information. Sli[illegible] ow[illegible] it [illegible] ef[illegible] o[illegible]s wh[illegible] h[illegible] ob[illegible] in[illegible] f[illegible] m[illegible] o[illegible] p[illegible] g[illegible] g[illegible] r[illegible] g[illegible] l[illegible] a[illegible] s[illegible] t[illegible] aling i[illegible] m[illegible] a[illegible] s[illegible]. Even so, it's [illegible] t[illegible] that [illegible] the most tech-savvy people can be victims of phishing attacks.

Be a cautious Internet user

- *Install a firewall.* This is the primary block between you and other computers on the network.
- *Install, run, and update antivirus and antispyware programs*. Visit *download.com* to check ratings of spyware removal programs.
- *Ensure your browser is up-to-date with security patches.* Set your computer to do so automatically.
- *Never use links within e-mail to visit a Web site.* Open a new browser window and type the URL (uniform resource locator) in the address bar.
- *Don't fill out e-mailed forms that ask for personal information.* The only way you should send credit card or account information is via a secure Web site—you'll see https (s for secure) and the padlock icon on the browser frame; click on the lock to view the security certificate.
- *Be cautious of and don't respond to urgent, upsetting, or exciting e-mails requesting personal information.* If a company or financial institution really needs to update your expired credit card number, for instance, you'll be a[illegible] take care of it[illegible] ne[illegible] you [illegible] a[illegible] tion[illegible] a[illegible] phone call you place to the company's customer service number on the card.



- *Be suspicious if someone claiming to be from your financial institution asks for confidential information.* This information should already be on file.
- *Review statements closely and report any suspicious activity to the source of the statement*. If you generally receive statements by mail, call the company if a statement is late to make sure an ID thief hasn't redirected your mail by changing your address.
- *If you have online access, monitor your accounts frequently*. That assures you'll notice unauthorized transactions promptly and can take steps to prevent more transactions.
- *Change your online banking and shopping account 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. Experts recommend