There's a new sport in town that involves some real poachers. It's call "phishing"-and the phishermen are trolling for you.

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.

Studies show that most identity theft still occurs when thieves obtain information from paper-by digging through trashcans or stealing from mailboxes. Even so, it's a fact that even the most tech-savvy people can be victims of phishing attacks.

Take these measures to help avoid becoming the "catch" of the day:

Be a cautious Internet user

. *Install a firewall as your first line* of *defense.* This is the primary block between you and other computers on the network. Also install, run, and update anti-virus and anti-spy-ware programs.

. *Ensure your browser is up-to-date with security patches.*

. *Never use e-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 *urgent e-mail requesting personal information.* Phony e-mails often include upsetting or exciting statements to get people to respond. . **Don't.** If a company or financial institution really needs to update your expired credit card number, for instance, you'll be able to take care of it the next time you make a transaction, or by a telephone 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.

. *Always review statements closely.* Report any suspicious activity immediately to whomever the statement is from. Most financial institutions and online companies will reimburse customers for any phishing losses. 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.

We will never send an e-mail

Request for personal information!
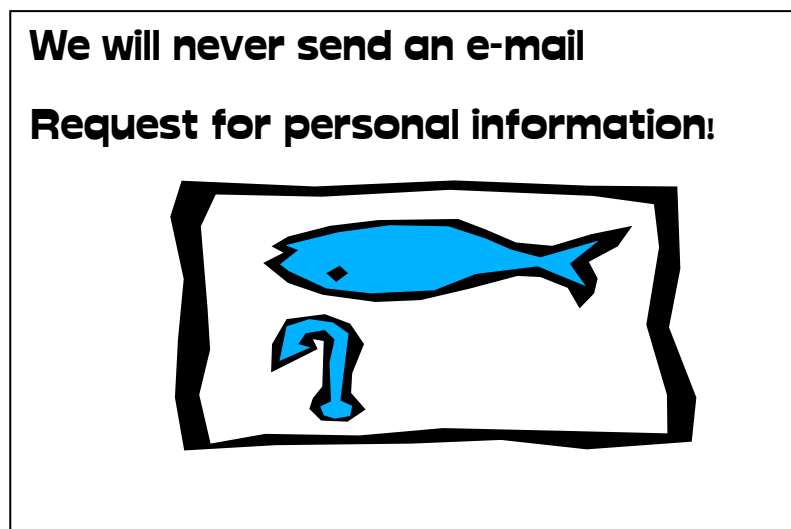
. *Change your online banking and shopping account passwords often-experts* suggest every three to six months. If your information is caught, your passwords should be out-of-date by the time crooks try to sell the data to other phishers. Experts recommend using passwords with a combination of letters (upper and lowercase), numbers, and symbols.

. *Request* a *free copy* of *your credit report from*

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 quick enough, you might be able to change your password or account number in time to stop unauthorized transactions.

This wasn't my idea of being a "Catch of the Day"

Phishing: Don't Take the Bait