

Financial U

Your Money,
Your Future

Brought to you by



Phishing Trip

Imagine you're a fish. You're minding your fish business, trying to get with some hot little guppy, when something irresistible drops in front of you. The succulent worm dangles before you as if someone or something placed it there intentionally. You circle around this "gift from above," carefully inspect it, and decide it's OK. You bite. All of a sudden a sharp pain rips through your jaw, and you're yanked out of the water struggling to breathe.

Next thing you know you're gutted, posing for some picture with some jerk you don't even know. Soon you'll be sizzling in some frying pan waiting for that same jerk to eat you—you've been phished.

Phishing is a form of identity theft that has gained popularity among hackers and criminals. So named because they cast the bait via e-mail and if you bite by opening the attachments or clicking the links, they can lure your personal information from you.

The link or attachment inside the e-mail sends you to a site that appears identical to the company's real site. You're asked to provide your username, password, account number—even your Social Security number.

The "spoofed" site looks exactly like that of an official company you're affiliated with, such as Best Buy, ebay, Amazon.com, or your own financial institution. But it's not—no legitimate business or financial institution will ever e-mail you and ask for personal identification information.

To avoid getting tangled in the net, follow these tips:

- *Don't respond to e-mails that ask for personal information, even if they look like they're from a trusted source.*
- *Don't e-mail personal or financial information, especially if it's through an e-mail request.* Contact your company over the phone or through the real—not spoofed—Web site. Call the company, ask for the URL, and bookmark it.
- *Don't click on any links or attachments in an unsolicited e-mail.* Again, close the e-mail and type the company's real URL when you need to contact the company directly.
- *Use a secure Web browser when submitting sensitive financial information over the Internet.* You can tell if a browser is secure by the padlock icon in the lower right-hand corner of the browser. Also, a secure Web site is indicated by an address beginning with "https" as opposed to "http."
- *Regularly review your accounts and immediately report any inaccurate information.*

If you receive fraudulent e-mail, forward it to spam@uce.gov and file complaints at ftc.gov.

For more information on phishing, go to antiphishing.org.



Nick Grube
UW-Madison senior
Journalism major
CUNA Intern



© 2005 Credit Union National Association
Brought to you by UW Credit Union
(uwcu.org) and America's Credit Unions.