



PHISHING EXPEDITIONS

WARNING: Be wary of E-mails that ask you to confirm your account information.

Here's a notice I received from PayPal asking me to update my account. When I clicked on the "Update your Information" link conveniently provided in the E-mail, it then asked me to enter my ID and Password in an official-looking PayPal form.

The problem was that the E-mail wasn't from PayPal at all, and the link opened a fake PayPal Web page. If I had entered my ID and Password, I would have given someone access to my PayPal account.

This is called "phishing," but the phisherman is collecting ID's and Passwords instead of fish.

There were three clues to this scam. First, the sender's E-mail name was "Service" and address was "reply_to@zidmaderdegsh.com" instead of "PayPal.com." Second, the message contained typos and punctuation errors. But most important, it asked me to click on the link provided in the E-mail, which is a no-no.

If you receive an unsolicited E-mail with a link directing you to log in to your on-line account, be very careful, or don't click it at all. If you need to view your account information, start your browser and enter the company's official address (URL) yourself, or use a bookmark you know is legitimate.

If you have any questions about unsolicited E-mails, please bring them to the PSRC computer lab on Tuesday from 1 to 4 p.m. or Friday from 10 to noon, and we'll help you figure out if they're for real. Otherwise, you could be on the "hook."

