

(Ph)ishing Is Not What It Used To Be

Don't get hooked by Internet scammers trying to find out your personal and financial information.

In the latest Internet scam, "phishers" send an e-mail or pop-up message that claims to be from a business or organization, such as your bank or federal agency. The message may tell you that you need to update your account information. You are then directed to a website that looks like a legitimate site, but it isn't. The only purpose of this site is to trick you into divulging your personal information. The "phishers" then use your personal information to steal your identity to run up bills in your name or commit other crimes.

These "phishing" scams can be carried out over the Internet or over the phone.

For example, you might open your e-mail one morning and find a message from your bank telling you that your account is overdrawn from a check that you didn't write. The message will urge you to take immediate action and will direct you to a website that looks like the website of your bank. They may even provide a phone number for you to call. When you call, the person on the other end of the line will tell you that he or she will take care of the matter while you're on the phone and then will ask for your social security number, bank account number and other personal information. Remember, if it is really your bank, they already have the information and you don't need to provide it again. By giving this information out, you have allowed these con artists access to your financial information to use to commit identity theft.

If you get this type of message, do not respond by e-mail or call the number that is listed. Take a few minutes to look in the phone book for the correct phone number or check your past statements for a



*Tips from your
Community Banker*

phone number and call your bank, credit card company or federal agency to see if there is really a problem.

A new emerging scam is called "pharming," whereby spyware is unknowingly installed on your computer. When you type in a legitimate URL (Universal Resource Locator) in your browser's address bar, a redirection scheme takes you to a fake website without you even knowing it.

The Federal Trade Commission suggests the following tips to help you avoid "phishing" and "pharming" scams:

- If you get an e-mail or pop-up message that asks for personal or financial information, do not reply or click on the link. Legitimate companies do not ask for this information via e-mail.
- If you initiate a transaction and want to provide personal or financial information, make sure the organization or business has a secure website.
- Use anti-virus software and keep it up-to-date. Anti-virus software and a firewall can protect your computer from accepting unwanted files.
- Report suspicious activity to the Federal Trade Commission. If you get spam (unwanted junk mail) that is "phishing" for information, forward it to spam@uce.gov. If you believe you've been scammed, file your complaint at www.ftc.gov.

***Provided as a public service by the
Pennsylvania Association
of Community Bankers.***