PHISHING

Don't take the bait!

Look for These Hooks to Spot a Fraudulent E-mail

"Verify your account."

» Businesses should not ask you to send passwords, login names, Social Security numbers, or other personal information through e-mail.

"Dear Valued Customer."

» Phishing e-mail messages are usually sent out in bulk and often do not contain your first or last name.

"Respond within 48 hours, your account will be closed."

» Messages that convey a sense of urgency are attempts to trick you into responding immediately without thinking.

» Phishing e-mail messages may claim that your response is required because your account might have been compromised.

"Click the link below to gain access to your account."

» HTML-formatted messages can contain links or realistic forms. The links are usually "masked," meaning that the link you see usually goes to a phony Web site.

» Resting (but not clicking) the mouse pointer on the link reveals the Web address. The cryptic string looks nothing like the company's true Web address, which is a suspicious sign.

» Con artisits use URLs that resemble the name of a well-known company that are slightly altered by adding, omitting, or tranposing letters.

What to Do If You Receive a Phishing E-Mail?

» Do not respond if you think you've received a phishing e-mail message.

» Report suspicious e-mail to the faked or "spoofed" organization. Contact the organization directly, not through the e-mail you received, for confirmation.

» Don't click links in fraudulent or suspect e-mail messages.

» Type addresses directly into your browser or use your personal bookmarks if you need to update your account information or change your password.

» Check the security certificate before you enter personal or financial information into a Web site.

» Don't enter personal or financial information into pop-up windows because there is no way to check the security certificate. Close pop-up windows by clicking the red **X** in the top right corner, not by using a close button within the message.

» If you notice suspicious activity report the incident to ***abuse@missouri.edu***.

Make it Safe

makeitsafe.missouri.edu

Division of Information Technology