

WHAT IS PHISHING?

In the field of computer security, phishing is the criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication. Communications purporting to be from popular social web sites, auction sites, online payment processors, IT Administrators or even the IRS are commonly used to lure the unsuspecting. Phishing is typically carried out by e-mail or instant messaging, and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one. Even when using server authentication, it may require tremendous skill to detect that the website is fake. Phishing is an example of social engineering techniques used to fool user, and exploits the poor usability of current web security technologies. Attempts to deal with the growing number of reported phishing incidents include legislation, user training, public awareness, and technical security measures.

BOTTOM LINE: If you get an email, instant message, or ANY other message from ANY other source requesting your personal info such as Credit card information, social security information, or ANY other personal information, chances are that email is a HOAX. DO NOT CLICK ANY LINKS! EVEN if they LOOK like they are legitimate. If you are concerned about your security on a particular site, visit that site directly by manually typing in the address to that website on your computer browser.

Version	Date	Author(s)	Comments
1.0	4/30/09	Eric Graves	