

A BRIEF GUIDE TO INTERNET FRAUD

© Copyright 2006 – David Todeschini
Conditionally released to public domain

WHAT IS PHISHING?

"Phishing" may sound like some ghetto slang word; possibly offensive but practically innocuous, but let me assure you - it is nothing of the sort. "Phishing" is a word coined in the Cyberspace vernacular after the proper English word "fishing" - and designed to be differentiated because what "Phishing" is, is analogous to casting a line into the water and catching a real fish.

"Phishing" is a crime - a crime of deception in which the "Phisher" (fisherman) casts his line out into the Cyberspace "sea", and inevitably comes up with a "fish" on his hook. This "phishing" usually takes the form of an E-mail - an "official-looking" E-mail from a bank, or from the ever-popular PayPal™ service. Usually the message will state that there is "a problem with your account", or asks you to "verify that you are the owner of this account", or requests to that effect.

The end-purpose of "Phishing" is to get the recipient of the E-mail to divulge a credit card number, account password, or other sensitive information about themselves, which will then be used by the "Phisher" to steal money from the victim's bank account, or run up credit card bills in his / her name.

BE OBSERVANT

In most browsers, when you move your mouse over a LINK, in the text, or a button on a web site, the URL (Universal Resource Locator) of where the link will take you, will be displayed on the bottom of the screen. Try it now. Move your mouse over the links below, and observe the URL at the bottom of your screen - then click on any of them, and see where they take you.

www.Google.com [Click on this link to verify your account.](#)

In the first example, what LOOKS like a link to Google, is actually a link to a demo page on THIS web site. Had I wanted to, I could easily have copied Google's web page, and made it LOOK LIKE you were actually on the Google search engine.

In the second example, the text in the link tells you NOTHING about where the link will take you. If you click on EITHER of the above links, they will take you to my demo page which could easily have been a Phishing scam.

In order to compare a REAL link to a fake one, try JUST moving your mouse over the two links below. Note that the TEXT in the links is IDENTICAL, but the first link will take you to my demo page if you click on it, and the second will take you to Google.

www.Google.com www.Google.com

Be careful to observe the URL bar at the bottom of your screen - if you move your mouse over the link (or the button), and the URL that appears is NOT where the link points to - you are probably looking at a Phishing scam.

Most banks and financial institutions will NOT solicit any verification information by E-mail. All reputable financial institutions deal in SECURE servers, and this can be verified by the prefix https instead of http in the URL when you are on their site.

WHAT TO DO IF YOU SUSPECT A SCAM

DO NOT respond to emails, or click on any links in e-mails that ask you for personal information, even if they appear to come from a legitimate source, and even if they contain information that only YOU would know - such as a partial Social Security Number, credit card number, etc.

DO NOT simply delete the E-Mail. First, forward it to the FEDERAL AUTHORITIES by forwarding the E-mail to spam@uce.gov. If you use AOL or another service that provides a "report spam" feature, go ahead and mark/report the message as SPAM. If you have a SPAM filter, you might want to include the message in the SPAM FILTER, so that you'll never get spammed from that sender again.

Finally, if you suspect that you have already been taken advantage of by "Phishing" or other online deceptions, or that your personal information is being fraudulently used by someone else, you can file a formal complaint at www.consumer.gov/idtheft .



This article is presented as a public service by author David Todeschini, and Net4TruthUSA
You may copy, e-mail, and post this article "not for profit" in any manner you choose, so long as it is posted in its entirety with all links intact. See www.Net4TruthUSA.com/CondCopyright.htm

