

Identity Theft: Gone Phishing

Article by: Daryl Campbell

Have you received one yet? You know. The email directing you to visit a familiar website where for some odd reason you're being asked to update your personal information? The website asks you to verify your passwords, credit card numbers, social security number, or even your bank account. You recognize the company name as one that you've done business with in the past, so you click on the "take me there" link and proceed to provide all the information they've requested. No problem right? Except you find out much later that the website is a fraud. It was created for one reason: to steal your personal information. Welcome to the world of phishing.

Phishing (pronounced as "fishing") means to send an email to a recipient falsely claiming to have an established, legitimate business. By fooling the recipient into giving their private information, the phisher has in effect stolen their identity.

It's not easy to spot an email phishing for information. At first glance, the email may look like it is from a legitimate company. The "From" field of the e-mail may have the .com address of the company mentioned in the e-mail. The clickable link even appears to take you to the company's website, but in fact, it is a fake website built to replicate the legitimate site.

Many of these people are professional criminals that have spent considerable time in creating emails that look authentic. Users need to review all emails requesting personal information carefully. When reviewing your email remember that the "From Field" can be easily changed by the sender. While it may look like it's coming from a company you do business with, looks can be deceiving. Keep in mind that phishers will go all out in trying to make their emails look as legitimate as possible. They will even copy logos or images from the official site to use in their emails. They also like to include a clickable link which the recipient can follow to conveniently "update" their information.

How do you check to see if the link is authentic? Point at the link with your mouse, and then look in the bottom left hand screen of your computer. The actual website address to which you are being directed will show up for you to view. This is a fast and easy way to check if you are being directed to a legitimate site.

Also never and I mean NEVER click the links within the text of the e-mail. Delete the e-mail immediately and empty the trash box in all of your e-mail accounts as well. If you are truly concerned that you are missing an important notice regarding one of your accounts, then type the full URL address of the website into your browser. That way you can be confident that you are being directed to the true and legitimate website.

Phishing is a major weapon of choice for online identity thieves. Don't get hooked. Daryl Campbell's website <http://fightidtheft.winthemarket.com> provides free tips, resources, featured articles from experts and up to the minute news concerning identity theft and fraud