

Identity Theft Article - A Phisher Is Trying To Steal Your Identity!

Article by: Lisa Smith

Sooner or later everyone with an email account will receive a phishing attempt from some internet scammer. What is phishing? How can you protect yourself? These are some of the questions this identity theft article will provide, along with some free resources and practical advice on how to protect your online identity.

The Anti-Phishing Working Group estimates that 75 million to 150 million phishing emails are sent every day on the internet. Phishing (pronounced fishing), is online identity theft that uses spoof emails, fraudulent websites and crimeware to trick unsuspecting internet users into providing financial data, credit card numbers, social security numbers, account logins and passwords, etc.

A spoofed email looks like it is from a legitimate company, usually banks, credit card companies, paypal, ebay, etc. These fraudulent emails look like they are from the "real" company, and generally try to get you to log into your account through the links in the email. The spoof email may state that there is a problem with your account and if you do not log in and update your information your account may be suspended, restricted, closed, etc. Generally these emails try to convey a sense of urgency; if you don't correct this problem your account will be suspended.

Trojans are increasingly being used as a phishing technique according to Sophos, a security firm. The Brazilian police recently arrested a phishing gang of 18 people who stole \$37M from online banking accounts. This phishing gang would send out emails that included Trojans. Once a Trojan infects your computer, all internet activity can be monitored and transferred to the phisher. This is a serious threat as you probably won't know that you are infected with a Trojan.

According to David Jevans, Chairman of APWG, "Attacks can, and are, coming in a variety of other flavors. Instant Messaging, exploited websites, P2P networks, and search engines are all being used to download and run key logging malware and/or be directed to websites which may contain malware or be fraudulent. Attackers are also not just interested in username and password access to bank accounts. Social security numbers, credit cards and other identity information are also being stolen."

Protecting yourself against phishing scams.

- Do not give out personal or financial information through an email request.
- Always log on to your sensitive accounts by opening a new browser and typing the actual URL directly into the address bar. For example, if you receive a suspected phishing email from ebay, open a new browser and type www.ebay.com in the browser bar.
- Do not click on any link in a suspected phishing email.
- Only use a secure website to submit sensitive data. A secure sites' address will begin with "https://" instead of "http://"
- Check the activity of your online accounts regularly.
- Make sure your browser is up to date and all security patches are installed.
- Report phishing and spoof email to: reportphishing@antiphishing.com , spam@uce.gov, and forward the email to the company that is being spoofed.
- Keep your pc protected with updated anti-virus software, anti-spyware software, and a firewall.
- You may also want to install anti-phishing software.

o Earthlink ScamBlocker is a free browser toolbar that alerts you to known phishing sites. It's free and can be downloaded at www.earthlink.net/earthlinktoolbar.

o Webroot has a beta version of PhishNet which you can download at www.webroot.com/products/phishnet/

o PC Tools Spyware Doctor offers protection against known phishing sites, spyware and blocks popups.

With the consequences being identity theft, it is imperative that you learn to protect your pc and your identity by exercising caution and installing the proper tools. Hopefully, this identity theft article has given you the information you need to avoid being the next phishing victim. Remember, legitimate companies don't ask for personal or financial information in an email – so don't give it to them!

Lisa Smith is the webmaster of 1stSpywareRemoval.com This website offers information on spyware, adware, internet safety, indepth reviews, and news.