

Internet Scams: Phishing

 <http://www.softwaretalks.com/phishing/>


There have always been scams. Get-rich-quick letters, pyramid schemes, fake competitions, charities that don't exist. The Internet hasn't increased the chance of falling prey to scammers - it just makes it easier for the scammers to get your attention. The tools available to senders of disreputable e-mail are extensive and cheap. Spam is illegal in many countries but we still get a lot of it. The same goes for the scams that arrive in our inbox.


These days, there are so many possible scams that it can be hard to tell the difference between them. The first we'll focus on is the practice of '**phishing**' - the word is derived from 'fishing' for consumer information, and 'ph' is a common replacement for 'f' in the hacking community. Phishing refers to the process of tricking you into giving up personal details such as your bank account or credit card details, or your passwords. Phishing is so prevalent on the Internet today that if you receive an e-mail purporting to be from your bank, it's likely to be either a criminal attempt to find out your login details and steal your money, or a real e-mail warning you to be careful of this phenomenon.

When I use my online banking service, I'm faced with no less than three separate warnings to ignore any e-mails claiming to be from my bank. At the same time I receive genuine e-mails from my bank, which themselves tell me to ignore e-mails from the bank. Another example is eBay, the popular web auction site. There was a time when eBay sent me regular e-mails about my account and the progress of my auctions. Now eBay urges their users to use an internal messaging system, akin to e-mails that only work when you're using the site, to communicate with the company. It's less convenient, but it is safer.

Due to the prevalence of this scam, most reputable companies, especially banks, will not ask you to take any direct action as a result of receiving an e-mail from them. They specifically request that you visit their company website directly and type in the address yourself, in order to seek more information.

Here's what to look out for. A phishing e-mail will often look and read like genuine material from a real company. So when you receive an e-mail from a company with whom you do business, think before you respond. Why did I get this e-mail? What is it asking for? Do I really need to take action now or can I verify it first? If the e-mail seems suspicious, for example if it's out of the blue, or contains spelling or grammar mistakes, you should check it before doing anything else by calling the company.


 You can also visit the website of the company, and login to check on your account, but be very careful not to click on any links from the e-mail. Through the use of pictures that look like **text links**, and also through the use of **IP addresses** (like 203.23.45.61) instead of regular web addresses, the e-mail changes where you end up but not the text that you see on the screen. Using this method, scammers can unknowingly redirect you to malicious sites. This is how they get people to enter personal details which are then sent over the Internet: not to your bank, but to criminals. The solution to this is easy - type the address you know, for example www.paypal.com, directly into your web browser yourself, and make sure you don't make any typing mistakes.

 There are also **e-mails** which clearly and simply request - for example - your credit card number, and some people do reply with these details. Just remember that you'll never be asked for such details in a legitimate e-mail.

A, B An interesting but rare form of phishing involves criminals purchasing a **misspelled website name**, for example www.payplal.com, and constructing a real-looking site designed to fool people. Only a small percentage of web users will incorrectly type the name, and less still might go on to enter their private details, but this can be enough for web bandits to make a tidy profit.

It's clear that banks and Internet giants are worried about the problem. But how concerned should we be, as Internet users? According to Gartner Research, phishing fraud between mid-2004 and 2005 cost over US\$2.4 billion. Phishing is big business. The good news is that prevention is not difficult. The popular and free Gmail service, from Google, includes a phishing filter that alerts you to most kinds of phishing e-mails. You can find an anti-phishing attachment on Microsoft's free MSN Toolbar and also in the next version of Internet Explorer (7.0). To report an e-mail or a site that you believe is a scam, you can visit www.antiphishing.com.

Technology can only help so much. The best defender against **phishing scams** is you. Take care when you receive e-mails and type in web addresses and remember, if in doubt: close your browser window or e-mail, and verify.

 **SoftwareTalks Podcast**
(Time 5:33 min; File Size 3.8 Mb)