



## Gone Phishing

Having written about passwords last month, it occurred to me that however good your passwords were, they would be of little use if you were “conned” into giving them up voluntarily. This is one of the areas of “cyber crime” that is growing rapidly, aptly called “Phishing”, and unfortunately more and more people are falling into the trap.

Wikipedia has a rather good description of Phishing:

“Phishers attempt to [fraudulently](#) acquire sensitive information, such as usernames, [passwords](#) and [credit card](#) details, by masquerading as a trustworthy entity in an electronic communication.... Phishing is typically carried out by [email](#) or [instant messaging](#), and often directs users to give details at a fraudulent website”.

How does it work? Phishers send out an email (to multiple recipients) that looks just like the email you would receive from your bank (for instance). It usually contains some sort of message relating to security or inactivity on your account, and then ask you to click a link and login to your account as usual. The trick is that you are not led to your bank’s actual website, but a fraudulent one that looks identical to your bank’s real site. You then login and the phishers have your bank login details...

85% of Phishing is directed at banks and other financial institutions, and is thus the form you are most likely to come across, though be aware that phishers will not just prey at banks, but will exploit other opportunities. A good example of this is following the Southeast Asian Tsunami in 2004, after which a variety of phishers decided to produce bogus websites of the world’s leading charities where kind hearted people could make donations to the relief funds using their credit cards.....

The APWG (the Anti-Phishing Working Group) is a useful source of information on the subject ([www.antiphishing.org](http://www.antiphishing.org)), alerting you to the latest scams and producing reports, including a few figures that indicate the size of the problem, such as:

- over 5 billion phishing emails sent each month
- unique fishing websites rose to over 55,000 in April 2007

- an increase of over 250% since the previous month!
- \$1,200 - average loss to each person successfully phished (Federal Trade Commission).

Most of the Phishing is directed at US Banks, but UK banks have not been immune to these scams, with Halifax, Lloyds, Barclays amongst others being targeted aswell. There is a test online that you can take to see whether you can recognise phishing emails at: [http://survey.mailfrontier.com/survey/phishing\\_uk.html](http://survey.mailfrontier.com/survey/phishing_uk.html) which includes some of the fake emails from UK banks, and also lets you see exactly what these emails look like. Incidentally, 92% of people who took the UK version of this test got at least 1 wrong answer.

The simplest advice against Phishing is (applies to banks, credit card companies, etc.):

- do not reply to any email from your bank – phone them instead
- do not click any links in an email from your bank
- if you think you have been had, inform your bank/credit card company immediately.

Over the last couple of months I have written about some of the security issues facing IT users today. This is not designed to put you of computers, but simply to make you aware that though spam and popup windows are annoying, there may be a more serious side to what turns up in your inbox. Next month: something a little more light-hearted.

Edward Marshall

Marshall Consulting  
21 Résidence St Martin  
Chemin des Faisses  
83300 Draguignan  
Mobile: 06 26 98 03 12, Tel: 04 94 84 12 90

[www.marshallconsulting.fr](http://www.marshallconsulting.fr)

© Copyright Edward Marshall 2007