



## Internet Scams - "Phishing"

July 2007

### Does something smell "phishy"?

**"Phishing" is a strange sounding term used in relation to a variety of Internet scams – it refers to a method of identity theft that often arrives via email. Our E-Business Advisers discuss how you can stay safe online:**

Fraud is a growing problem on the Internet, as people are tricked into providing personal information including credit card numbers, passwords, key words and bank account numbers.

Virus protection and firewall software often fail to catch phishing scams, because they do not contain suspect code, while spam filters let them pass because they appear to come from legitimate sources.

#### 1. What happens?

You receive an innocent looking email that appears to come from a legitimate source, such as a trusted business or financial institution.

It includes an urgent request for personal information, usually invoking some critical need to update your account immediately. Clicking on a link provided in the email takes you to an official-looking web site where they invite you to update your personal information.

Sadly, however, your personal information is then captured, and stored on a database which is held by the scam artist.

The links included in phishing scams take the unsuspecting person to a fraudulent web site

designed to mimic the real thing, often down to the smallest detail including copyright notices, submenu titles and so on.

It's very difficult for most people to tell they are the target of a "phisher" by looking at the site alone.

#### 2. How can you tell it's a bogus web site?

Clues in the web site address can sometimes reveal the deception. Similar looking characters might be substituted in the spelling of the link for the real character so that a "1" (numeral one) is used in place of a lower-case "L." For example, phishers have used paypa1.com rather than paypal.com.

Other times an Internet Protocol (IP) address – (a numerical address used by the Internet to denote location of a web site etc) – is used to hide the fact that the link is not taking the victim to the real site.

However, phishing scams have become so sophisticated that phishers can also appear to be using legitimate links, right down to the real sites' security certificates.

#### 3. Key tips for protecting yourself and your company

1. Never respond to emails requesting personal/financial information

Banks or e-commerce companies generally personalise emails, while phishers do not. Phishers often include false but sensational



# Fact Sheet

messages ("urgent - your account details may have been stolen") in order to get an immediate reaction.

Reputable companies don't ask their customers for passwords or account details in an email. Even if you think the email may be legitimate, don't respond - contact the company by phone or by visiting their web site.

Be cautious about opening attachments and downloading files from emails, no matter who they are from.

## 2. Visit Bank web sites by typing the web site address in yourself

Phishers often use links within emails to direct their victims to a "spoofed" (i.e. faked) site, usually to a similar address such as mybankonline.com instead of mybank.com. When clicked on, the address shown in the address bar may look genuine, but there are several ways it can be faked, taking you to the spoofed site.

If you suspect an email from your bank or other company is false, do not follow any links embedded within it.

## 3. Keep a regular check on your personal and business accounts

Regularly log into your online accounts, and check your statements. If you see any suspicious transactions, report them to your bank or credit card provider.

## 4. Check the web site you are visiting is secure

Before submitting your personal, bank details or other sensitive information, there are a couple of

checks you can do to help ensure the site uses encryption to protect your personal data:

Check the web address in the browser address bar. If the web site you are visiting is on a secure server it should start with "https://" ("s" for security) rather than the usual "http://".

Also look for a closed padlock icon on the Internet Explorer web browser's status bar - at the bottom of the screen. You can check the level of encryption, expressed in bits, by hovering over the icon with your cursor.

However, the fact that the web site is using encryption doesn't necessarily mean that the web site is legitimate. It only tells you that data is being sent in encrypted form.

## 5. Be cautious with emails and personal data

Most banks have a security page on their Web site with information on carrying out safe transactions, as well as the usual advice relating to personal data.

Never let anyone know your PIN or password, do not write them down, and do not use the same password for all your online accounts.

Avoid opening or replying to spam emails as this will give the sender confirmation they have reached a live address. Use common sense when reading emails. If something seems implausible or too good to be true, then, as always, it probably is.

## 6. Keep your computer secure

Some phishing emails or other spam may contain software that can record information about your Internet activities (spyware) or open a 'backdoor' to allow hackers access to your computer (Trojans).



# Fact Sheet

Installing anti-virus software and keeping it up to date will help detect and disable malicious software.

It is also important, particularly for users with a broadband connection, to install a firewall. This will help keep the information on your computer secure. Make sure you keep Microsoft products up to date, and download the latest security patches for your browser.

## 7. Always report suspicious activity

If you receive an email you suspect isn't genuine, forward it to the organisation whose web site has been spoofed (many companies have a dedicated email address for reporting such abuse).

## 4. Some examples of "Phishy" tales....

In early April 2005 an email appearing to be from Microsoft urged recipients to download a much anticipated security update. Those that clicked on the link in the email were taken to a site that looked like a legitimate Microsoft update site.

However, instead of updating their software, they were actually downloading a Trojan horse (a remote access program that can steal personal information). Microsoft does not use email notification in this way - but many were caught unaware.

The famous "letter from Nigeria" is another type of phishing scam, and has been around since before the Internet!

This type of scam is so prevalent, it has its own name: the 419 scam, which refers to a section of the Nigerian Penal Code. The phisher pretends to be a Nigerian official in distress requiring a personal bank account to offload money.

The person who allows temporary use of their account would receive a handsome reward. Instead, those who provide their banking information become victims of theft.

There are many variants on this theme, by no means all originating from Nigeria. The authors saw several cases of a particularly disgraceful example after the Paris "Concorde" air crash.

The email, purportedly originating in Rumania, said that a German family, who had all (genuinely) died in the crash, had left a large amount of money in a German bank account, and Rumanian relatives were having difficulty in getting the bank to pay this money to them as they weren't (then) within the European Union...

If you gave them your UK bank account details, they could get the money out via your account - and (obviously) handsomely reward you. Truly a disgusting scam....but there are many other equally distasteful examples, unfortunately.

Research firm Gartner Group found phishing scams are costing consumers & businesses around \$2 billion a year. Catching phishers is difficult, because these "phishy" Web sites operate for very short periods of time, and scams are often run from countries with lax legal structures.

The Anti-Phishing Working Group (APWG) is an international organisation of volunteers working to track phishing scams. Their Web site keeps an online database of fraudulent emails submitted to them. You can check this site for new scams, or send them phisher email you receive.



# Fact Sheet

## 5. Useful Links

[www.banksafeonline.org.uk](http://www.banksafeonline.org.uk) -  
Information published by the British banking industry, on how to protect yourself against online fraud.

[www.antiphishing.org](http://www.antiphishing.org) -  
Web site of the Anti-Phishing Working Group (APWG)