

## Phishing

Phishing - someone with a lisp trying to catch a fish? No, it's much more serious, potentially financially devastating. We've all heard of e-mails that try to get you to give your credit card number and pin numbers – these e-mails are “phishing” for your personal information so that it can be used for identity theft or financial crimes.

How do they work and how can you protect yourself from them?

Phishing authors send e-mails that look as if they come from your bank or other on-line financial institutions (such as PayPal or Ebay) requesting you re-enter or verify personal information from you. Included in the e-mail will be convenient links to their web site. These links will look like the correct address, but they are just pictures. Underneath the picture, hidden from you, the user, is the actual link to their web site. Thus, when you click on this pseudo link, you get transferred to a bogus site, where your information (if you enter it) is harvested from you and the next thing you know is that your bank account is empty, your credit cards have reached their limits and your identity has been spoofed.

Reclaiming your true identity is much more difficult than you might think. Whilst it is easy to go to the bank with physical proof, trying to regain your credit rating or, even worse, getting your name off the FBI most wanted list (remember Mr Bond, detained in South Africa because his name was on the FBI list?) is next to impossible. The information that the fraudsters want is data that the actual institution should already have and would never ask you for via an e-mail. So how do they get people to give this information when, in the cold light of day, none of us would fall for their tricks? A typical ploy is

to “scream” at you that your account is about to be closed, or that some fraud has been committed and they need some verification. In our increasingly busy life, when we see this we panic. Also, these warnings may arrive outside office hours, so we feel we cannot contact the relevant institution to check.

What should you do? Firstly, don't panic, use common sense and remember the old saying Act in Haste, Repent in Leisure! No financial institution will ask you for information this way. Most of the information they already hold and they will contact you by phone (never e-mail) and ask you questions to identify yourself before discussing account details. Secondly, never *ever* click on the links within the e-mails. If you want to check if the e-mail is from who you think it is, re-type the link into your web browser (don't copy or you might copy the fraudulent link instead of the original). Alternatively, call the institution, but don't use the number on the e-mail – it too will be fraudulent and could well be a premium rate number (more money from you!). A variation of this targets businesses. It is a variation of the good old Nigerian Scam. A supposedly high up official/academic/professional in Nigeria has got a bucket load of money but it is trapped in Nigeria and they need your help (why you?) to get it out. What they need is your bank account details so that they can put the money directly into it and then you will move the money (less a hefty commission – enough for you to retire on) to another account (details of which will follow after the transaction has occurred). Oh dear, that's your bank account empty! If you don't fall for this they say that they need a sum (say £5,000) to “ease” (hint hint, wink wink) the progress of the money out of Nigeria. Once you have paid this money into some foreign account, off they go never to be seen again.

Sadly, these scams must work as the Nigeria Scam has been going for over 30 years. The best defence is a good dose of common sense and scepticism about any unusual e-mails

---

## First Contact

### Addresses and phone numbers

Looking up phone numbers and addresses is so easy on the Internet. BT has an online directory enquiries service for both residential and business numbers. Go to [www.118500.com](http://www.118500.com) The cost is just the cost of your internet access. You can also find business numbers at [www.118888.co.uk](http://www.118888.co.uk). If you are looking for business numbers in a particular area, try using the internet version of Yellow pages at [www.yell.co.uk](http://www.yell.co.uk)

Mislaid that all-important postcode? Go to [www.royalmail.com/portal/rm/postcodefinder](http://www.royalmail.com/portal/rm/postcodefinder). You have to register to use this service but it is free. Alternatively, if you know the postcode but not the full address, try visiting <http://pol.royalmail.com/dda/AF.asp>

Finding someone's e-mail address from their name alone is not so straightforward. The best way is to install Copernic Agent Basic, which is a free download from [www.copernic.com](http://www.copernic.com) that does a super search of the web. Type in the name you are looking for in the Search For box and in the Category box, double click on Favourites/E-mail addresses. Click on All the Words in the Search box and click Search. It's not infallible but it's worth a try.

---

## Spamming update

US firm Savvis, which describes itself as "the network that powers Wall Street" has been forced by Steve Linford, who runs the Spamhaus black list, to get rid of spammers using its network. It is alleged by a former employee, that Savvis could have been earning up to \$2m per month from these spammers (Savvis claim it was just a tenth of this figure).

The Spamhaus project maintains free list of spammers IP addresses. This list is available to e-mail administrators and users in order to block incoming spam. It is updated hourly through 32 servers throughout the world.

Until this year, Savvis was considered a model service provider, strongly against spammers. However, when it bought Cable & Wireless, they inherited 95 major spammers. Since the purchase in January, it is estimated that another 53 have been added.

Savvis have responded in a very positive fashion by dropping these spammers immediately. Sadly, all that will happen is that they will go to another, more unscrupulous ISP - \$2m per month is a lot of money! The volume of spam is still increasing, MessageLabs scans 65m e-mails daily and found that up to 84% are spam!

---

## Manipulating Windows

### Cascading

If you have opened several files and you need to work between them, they will be easier to see and manipulate if you cascade them.

- Right click on an empty part of the Taskbar at the bottom of your screen. Choose Cascade Windows
- Click on the blue title bar of the window you want to bring to the front.
- To move a window out of the way, click on the title bar, hold the left mouse button down and move the mouse till the window is in the required position.
- To clear up in one click, hold down the SHIFT key and click on the File menu of the front window. Click on the Close All option. You will be prompted to save your changes if you haven't done so already.

---

## Eradicate those Scratches

The data on CDs and DVDs is stored on the surface and so scratches can cause the laser that reads them to misunderstand the information. Help is at hand from Scratchbusters who use a fine sanding machine to remove the top layer of the disc. Repairs cost between £2.50 and £4.00. If repair is not possible, charges will be refunded [www.scratch-busters.co.uk](http://www.scratch-busters.co.uk)