

# Something **phishy** in the net

While it may take years to build a name, it only takes seconds to steal one through a form of Internet fraud known as phishing – the online version of identity theft.



By **CLAIRE JONES**  
Manager, Little Black Dress

**Phishing isn't really a new concept. Long before the advent of personal computers and the Internet, the same malicious characters were tricking unsuspecting consumers into providing their personal details over the phone. This practice was called social engineering and still exists as a weapon in the scammer's arsenal to this day.**

Phishing is the contemporary version of an old crime – the intent is the same but the process now involves spam and phoney web pages.

In its typical form, phishing involves the dispatch of an e-mail purporting to originate from a legitimate organisation such as a bank or Internet Service Provider, which asks the recipient to verify their personal information such as account numbers or passwords. The e-mails may look authentic and often mimic the design and style of the real organisation's website, complete with the official company logo and cleverly masked hyperlinks that appear to connect to the genuine corporate website – the problem is, they don't.

The sender usually asks recipients to confirm their account details to avoid imminent closure, or to replace information that's been lost due to a database malfunction, or to allow them

to verify an order that's been placed in the recipient's name.

Some of the more audacious scammers pretend to represent the fraud departments of various institutions and governments and ask recipients to verify or supply their personal details because they suspect the recipient has been a target of online identity theft. There's even a reported case of a phisher who claimed to represent the state lottery commission and asked recipients to confirm their account details so that he could deposit their winnings. These e-mails make for compelling reading to the uninitiated, and it's little wonder that so many have fallen prey to online fraud.

The increase in phishing attacks has resulted in a push by the Australian finance sector for a review of current liability provisions which would see customers who fall victim to Internet scams responsible for wearing some of the cost.

Under the current *Electronic Funds Transfer Code of Conduct*, financial services providers are usually liable for unauthorised third-party transactions. However, in a recent discussion paper released by the Australian Securities and Investments Commission, the question of whether customers should

be held partly responsible is an issue earmarked for review.

While some argue that the cost to the finance sector of phishing attacks is significantly outweighed by the savings derived through the move from traditional to electronic banking by thousands of customers, the notion of shared responsibility – particularly in cases where the customer has responded to a phishing lure with "extreme carelessness" – is gaining momentum.

That being the case, it's more important than ever to ensure your personal details remain personal, and to protect that which is often the hardest to regain – a good name and credit rating.

From a business perspective, the increase in phishing attacks has dampened the enthusiasm of some consumers to conduct business via the Internet, which is bad news for any organisation whose revenue growth is linked to an increase in online transactions.

#### **Don't take the bait!**

Unless you plan to cancel your e-mail account, swear off online shopping and revert to banking with passbooks and paper statements, it's almost impossible to avoid the odd phishing attack from

opportunistic scammers. But there is a lot you can do to protect yourself and become a savvy Internet user.

- Legitimate businesses rarely, if ever, ask for personal information via e-mail. If you receive such a request, call the organisation for confirmation or check its legitimate website, but make your own way there, ie don't follow a website link from within the e-mail. Open your browser and type the web address yourself.
- Look for misspellings and bad grammar.
- If the e-mail refers you to a web site, look carefully at the URL. It's easy to disguise a link to a phoney site by using the @ symbol in a web address. Russel Kay, a writer with Computerworld explains: "Most browsers will ignore anything preceding the @ symbol, so www.business.com@phoneysite.com may look like a page from the business site, but it actually takes visitors to "phoneysite.com". The longer the URL, the easier it is to conceal the true destination address. Other ways to disguise URLs include substituting similar-looking characters, so that paypal.com could be (and has been) spoofed as

## Case in point:

On 17 November 2003, hundreds of eBay customers received e-mail notification that their accounts had been compromised, which would result in trading restrictions or closure. The message contained a hyperlink to what appeared to be an eBay Web page where they could re-register. The top of the page looked just like eBay's official home page, complete with all the internal links. To re-register, the customers were told they had to provide credit card data, ATM personal identification numbers, Social Security number, date of birth and their mother's maiden name.

Over a period of almost a year, Matthew Guevara developed fake e-mail messages using a Hotmail account and a fraudulent website through Yahoo! with the seemingly realistic domain www.msnbilling.com. Guevara asked MSN customers to verify their accounts by providing their name, account details and credit card information. Guevara pleaded guilty to wire fraud and faces up to five years imprisonment and \$250,000 in fines.

Between July and December 2002, a 17-year-old California boy set up an elaborate e-mail and website purporting to be run by AOL. He e-mailed AOL customers warning of account closure if they did not update their billing information. The minor conveniently provided a link that supposedly connected users to the AOL Billing Center, but actually connected to a site hosted by the boy who fooled his victims into providing credit card numbers, mothers' maiden names, billing addresses, social security numbers, credit limits, PINs and AOL passwords. This clever teenager didn't just steal one credit card number from his victims, but two! After asking the AOL customer to enter their credit card used by AOL for billing, the website told the user to enter new credit card information to correct the supposed billing problem. He then used the credit information to purchase goods, along with the victims' AOL e-mail accounts to send out more fake e-mails. He was eventually caught and prosecuted and ordered to repay all his ill-gotten gains.

paypal.com or paypa1.com. Similarly, a zero can be substituted for the letter O within a URL."

- Install anti-virus software and update it regularly to ward off "pharming" attacks, another form of online identify theft where a virus or malicious program is secretly planted in your computer to hijack your web browser. When you type in the address of a legitimate web site, you're taken to a fake copy of the site without knowing. This allows the pharmer to steal any personal information you provide at the phoney site, such as your password or account number.
- Be wary of entering personal information into a pop-up screen. Phishers may direct you to a legitimate company's web site, only to be presented with an unauthorised pop-up screen created by the scammer. The pop-up contains blanks in which to provide your personal information which is then routed directly to the phisher.
- Make use of spam filters to limit the number of phishing e-mails you receive, along with anti-virus and anti-spyware software, which help protect against pharming attacks and unauthorised programs that track your online activities without your knowledge. Guard against hackers and unauthorised communications with firewalls, which is important if you have a broadband connection, because your computer is open to the Internet whenever it's turned on.
- Practice caution when opening e-mail attachments. The general rule is to only open an attachment if you're expecting one and/or you know the sender and what the file contains. Phishers use attachments to send viruses and spyware programs which are triggered to run when opened.
- Remember that identify theft isn't just a problem for web users. Scammers may contact you by telephone pretending to represent a reputable company or government agency, and ask you to verify or supply personal information. If in doubt, take the caller's name and number, and then contact the organisation in question to verify the person's legitimacy.
- If you do get hooked by a phisher, take immediate action. Notify the company in question of the incident and ask them to cancel your account.