AICrime Reduction Matters

Australian Government
Australian Institute of Criminology

No. 37 1 September 2005

Reducing the risks of 'phishing'

'Phishing' is a term that describes a way in which a person using the internet may be tricked into giving their personal identification information or banking and finance details to a criminal. Once this information has been obtained by a phisher, they may sell it to another person or use it to commit identity fraud. Internet users need to be aware that credit card details or log-in details used to access finances and services online are valuable and can be misused by others. Phishing is not limited to email-scams. There are three types of phishing attack, depending on whether the attack uses human nature, technical exploits or a combination of both.

1. Attacks based on human nature are sometimes known as 'social engineering'. An example is spam email requiring a person to 'validate' their credit card or internet banking account log-in details by replying to the email.

2. Technical exploits may also be used against machines without a person giving away information. Examples are password sniffers that can be used to intercept encrypted passwords travelling over a network. Other technical ploys include: Internet Protocol (IP) spoofing, 'Trojan horse' software and key logging.

3. Technical ploys and social engineering come together in cases such as a 'man in the middle' attack where a hacker routes messages between a vendor and client through a bogus web site that mimics the vendor's. Other attacks that combine human nature and technical disguise are false web sites that rely on domain name service (DNS) poisoning, 'DNS hijacking', and cross-site scripting to hijack web users. Such attacks that do not require a user to respond to a lure are sometimes referred to as 'pharming'.

The risks of 'phishing' can be reduced if the following measures are followed:

- Never provide personal details, including customer ID or passwords, in response to any e-mail. A bank or other financial institution will never ask you for your private password. This important information should never be shared with anyone.
- Never click on a link or attachment in an e-mail which purportedly sends you to a bank's website. Only access your bank's Internet banking logon page by typing the address into your browser.
- Be wary of any e-mail from someone you do not know or trust. Delete without opening any e-mails that you think are suspicious.
- Always check your bank statements for any transactions that look suspicious. If you see a transaction that you did not make, immediately report it to your bank.
- Most 'phishing' e-mails do not address you by your proper name because they are sent out en masse. They sometimes contain typing errors and grammatical mistakes, even if they include a bank's registered logo.
- Install software that will filter spam e-mail or use an Internet Service Provider (ISP) that will filter spam prior to delivery at your Inbox. Spam filters are often included in anti-virus software.
- Regularly download and install security patches for your operating software. Install, update and use anti-viral software.

Further reading:

Krone A 2005. Phishing *High tech crime brief* no 9. Canberra: Australian Institute of Criminology

Australian Bankers Association & Australian High Tech Crime Centre 2005 *Protecting your information online fact sheet* http://www.ahtcc.gov.au/MediaReleases/fact_sheet_PYIO.pdf