Australian Government
Australian Institute of Criminology

AUSTRALIAN HIGH TECH CRIME CENTRE

High Tech Crime Brief

2005

09

Phishing

Identity crime and phishing

Phishing has emerged as a major problem on the internet. The object of phishing is usually to obtain information about people in order to commit fraud. Phishing fits within a broader category of identity crime in the digital age.

The play on words with fishing is deliberate – the term connotes the speculative baiting of victims in order to get them to reveal details of their online identity. The overarching concept is one of using digital means that rely on either human or technical vulnerability, or both, to trick online users into divulging information or do things that they would not do if fully aware of the consequences. However, the term also encompasses ways in which computers can be manipulated to provide information or transfer value without requiring a human response.

Phishing is a function of the expansion of online commerce where face-to-face transactions are not necessary to buy goods and services, to transfer value, or engage in transactions that regulate aspects of identity. This provides the opportunity for criminals to commit fraudulent acts in the following ways:

- pretending to be another person online and abusing that person's existing credit or debit facility;
- pretending to be another person in transactions with that person's bank or other financial service provider; and
- assuming the identity of another person and using that assumed identity to incur debts and liabilities in that name.

In order to commit an offence using someone else's identity online, an offender requires information about the means of authenticating the online identity of the other person. Depending on the offence, this may include information about the victim's credit card details or the victim's log-in details when dealing with their finances online.

Estimates of email-based phishing

The Anti-Phishing Working Group (APWG) provides the most comprehensive picture of the scale of email-based phishing attacks on the internet. There were 13,141 new unique phishing emails identified in February 2005. While 64 brands were targeted, six brands accounted for 80 per cent of phishing campaigns. The growth in reports to the APWG of phishing email is shown in Figure 1. This shows a dramatic rise from 107 emails reported in December 2003 to 13,141 emails reported in February 2005. Many of these emails would be captured by anti-spam software where such software is in use.

There were 2,625 separate phishing sites reported in February 2005. These were maintained for short periods with an average time online of 5.7 days. The APWG infers that the number of machines being compromised and used to host phishing attacks continues to grow based on the changes over time in the computer access ports being used to launch attacks. Most phishing sites in February 2005 were hosted in the United States (37%), followed by China (28%), Korea (11%), Brazil (3.9%), Germany (2.9%), Japan (2.4%), Canada (2.2%), Argentina (1.7%), France (1.7%) and Romania (1.4%).

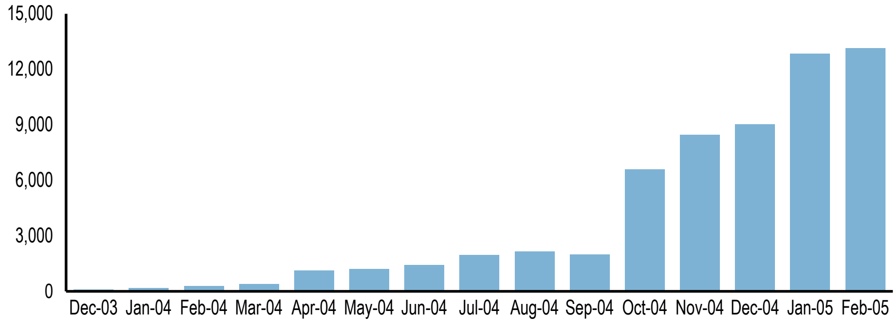
Types of phishing attacks

Phishing is not limited to email-based attacks. There are basically three types of phishing attack depending on whether the attack uses human nature, technical exploits, or a combination of both.

Attacks based on human nature

Attacks based on human nature rely on the capacity to use digital communication to manipulate other people to divulge information and data or to allow physical access to areas that a person is not entitled to, by using social dynamics. This is sometimes known as 'social engineering' which is really a new name for various forms of fraud, or confidence tricks that do not of themselves necessarily directly involve monetary loss, but which compromise the security or integrity of digital information or the physical security of such information. An example is spam email requiring a person to 'validate' their credit card or their internet banking account log-in details. Attacks that

Figure 1: Growth in reported phishing attacks



Source: APWG 2005

rely on just this level of sophistication can be wide-cast, using spam emailing techniques, or may be targeted to specific individuals.

Attacks based on technical exploits

In other cases, technical exploits are used against machines without necessarily involving a person in divulging information. Examples are password sniffers that can be used to intercept encrypted passwords passing over a network and password crackers that can be used to decrypt passwords or try out multiple combinations of passwords to circumvent password security measures. IP spoofing can be used to gain access to a network by packaging a message to another computer as being from a trusted source. A victim's computer may also be infected by 'Trojan horse' software that allows a hacker to gain privileged access to the computer and, for example, to capture and relay the keystrokes of the victim to the hacker's computer. Keylogging is sometimes referred to as 'ghosting'.

Attacks based on human nature and technical exploits

Very often the combination of technical ruse and a play on human nature come together in more sophisticated examples of phishing. In particular, offenders use the technical ability to manipulate applications on the internet to make them appear to potential victims as something they are not. An example is the spoofing of an email address to make the email appear to originate from the email address of another person or business. In a 'man in the middle' attack a hacker routes messages between a vendor and a client through a bogus web site mimicking that of the vendor. The offender is then able to capture account information that is relayed in the online transaction without being visible to the client or the vendor's computer.

Other attacks that combine human nature and technical disguise are false web sites that rely on domain name service (DNS) poisoning, which allows an offender to portray a false site on the internet as a legitimate site and attract messages that would ordinarily be conveyed to the legitimate site. DNS cache poisoning occurs when an attacker hacks into a domain name server, then 'poisons' the cache by planting counterfeit data in the cache of the name server. When a user requests a site by typing in its name, the IP address is resolved by the hacked domain server, and the bogus data is fed back to the browser. Another tactic, dubbed 'DNS hijacking', is similar, but simply changes the domain server so that traffic is actually re-routed (Keizer 2005). The APWG (2005) reports that in January 2005 a number of phishing attacks used cross-site scripting to redirect URLs from popular web sites in order to better present themselves and to prevent blocking. Attacks such as this that do not require a user to respond to a lure are sometimes referred to as 'pharming' (Roberts 2005).

Responses to phishing

Early versions of phishing email were characterised by spelling and grammatical errors and were often not made up to look like messages from the institution being impersonated. There has been much publicity given to the problem of unsolicited email being used for criminal purposes. It is to be hoped that consumers now heed the message not to respond to an email that seeks to verify or confirm their online authentication details. There has been a steady transition from one-off attacks dependent on response to email to persistent attacks using redirection or malware techniques that may trap otherwise astute internet users. The responses to phishing need to reflect this change.

An important threat to emerge is the use of spoofed embedded links that look like links to the institution being impersonated but which lead to malicious sites. In response to this threat users have been warned not to use embedded links in email purporting to be from financial institutions. However this warning is powerfully undermined where some financial institutions persist in emailing customers with messages containing embedded links for the customer to do anything related to their account. This creates an opportunity for criminals to distribute copycat email with spoofed links that divert customers to malicious sites or that can load Trojan horse software on to the customer's computer.

The development of technical attacks poses a growing challenge. Unlike email-based attacks that are relatively short-lived, these attacks tend to be more persistent, are often difficult to detect and once detected require the development of a patch that is then implemented by the computer user. One writer has cautioned that the reactive approach of addressing each phishing attack as it is identified provides inadequate protection. He calls for the development of ways of detecting and blocking changes in IP address resolution systems (De La Cuadra 2005). Two-factor authentication, where more than one process is required to be identified online, may also remove the incentive to phish.

How to protect your information online

A fact sheet on how to protect your information online has been developed by the Australian High Tech Crime Centre with the Australian Bankers Association and can be found online at http://www.ahtcc.gov.au/MediaReleases/fact_sheet_PYIO.pdf

Contact
Australian Institute of Criminology
GPO Box 2944 Canberra ACT 2601
Phone: 02 6260 9200 Fax: 02 6260 9201
Web: www.aic.gov.au

Project no. 0074 ISSN 1832-3413

The Australian High Tech Crime Centre funded this research

Further reading

Anti-Phishing Working Group (APWG) 2005. *Phishing activity trends report* http://www.antiphishing.org/

De La Cuadra 2005. *Pharming – a new technique for internet fraud*. eChannelLine Canada http://www.crime-research.org/news/07.03.2005/1015

Keizer G 2005. Possible domain poisoning underway. *TechWeb news* http://www.techweb.com/wire/security/60405913

Roberts P 2005. DNS pharming attacks target.com domain. *Computerworld* 1 April 2005

Disclaimer: This research paper does not necessarily reflect the policy position of the Australian Government, the AIC or the AHTCC