Identity Theft and "Phishing"

PROFESSOR MARK GRIFFITHS*

Recent research by the UK's National Hi-Tech Crime Unit (NHTCU) shows that cybercrime costs the country billions of pounds. In a survey of 201 companies, 167 firms (83 *per cent*) said they had suffered some sort of computer crime in the past year, costing them £195m, with 62 *per cent* losing a total of £121m to Internet fraud (Cowan, 2004). Furthermore, of 44 financial services businesses polled, three alone totalled fraudulent losses of £60m. Virus attacks were experienced by 77 *per cent*, costing them £27.8m, and 17 *per cent* lost £23m to criminal use of the Internet, mostly by employees, who sabotaged data and networks. Some 11 *per cent* had data stolen and *15 per cent* had had spoofs made of their corporate web sites (Cowan, 2004).

More specifically, identity theft – where criminals create false accounts in someone's name – is fast on the increase. According to the latest figures supplied by the Association of Payment and Clearing Services, card fraud involving identity theft rose by 45 *per cent* last year to a record £29.7m (O'Hara, 2004). "Cardholder not present" (CNP) fraud, increased by six *per cent* and accounted for the greatest part. CNP fraud typically involves the unauthorised use of stolen card details through payments by telephone, Internet and mail order. The card industry and police are hoping the introduction of new "Chip and Pin" technology, where an identification number replaces signatures, will tackle CNP in particular.

The three most popular ways used to get hold of card numbers are: (i) skimming, where the information stored on the magnetic strip of a card is duplicated and copied to a replica card, (ii) stealing details from card statements discarded in bins, and (iii) "phishing" where e-mails are sent in the hope that recipients reveal their personal financial details. Another highly sophisticated (but less popular) method of obtaining passwords and financial account details are the use of remotely operated key-logging programs which record and download the key-strokes that users make when typing. Thankfully, most banks have switched their logging-in procedures for online customers to avoid the threat from these programs. Instead of requiring customers to type in their passwords and identities, the banks are making customers click on a "drop-down" menu or alphabet by clicking on it with their mouse.

With regards to identity theft, "phishing" appears to be causing the most concern since its introduction to the UK in August 2003. Phishing – a term derived from the way computer thieves go fishing for private data on the Internet – involves the use of junk e-mails sent out randomly to lure unsuspecting victims to bogus web sites where they are fooled into typing in their account details and passwords as a security precaution. For instance, here is a verbatim e-mail that thousands of people received which pretended to be from Barclays Bank:

"Hello dear client Barclays Bank. Today our system of safety at night has been cracked!!! It not a joke!!! It is the truth!!! We ask you, in order to prevent problems, to repeat registration of your data. Make it very quickly! Administration Barclays Bank." (sic)

Even these apparently crude messages have caused people to divulge their online banking passwords to organized criminals. Those who responded and logged onto the address in the *Barclays* e-mail (above) found a web site that looked virtually identical to the bank's site. Brands and logos are the touchstones that people rely on to decide who and what to trust. If a bank customer types in their card numbers and security codes as requested in the e-mail, the fraudsters then access the victims' accounts and transfer money into the accounts of British mules. They then withdraw the cash and wire it out of the country in return for a cut of about five *per cent*.

Because fraudsters cannot obtain lists of customers, they speculatively target the most popular banks (eg, *Lloyds TSB, Natwest, Barclays,* etc), on the assumption their strike rate will be higher (Bowcott, 2004a). Hackers in Eastern Europe have learnt how to disguise an e-mail address by hiding additional letters or characters that would expose its true location. Scam e-mails are often link to web sites that differ by only one character from the *bona fide* site. In the US, there is a similar situation. *EBay* is the most spoofed site, followed by *Citibank, AOL, PayPal, EarthLink, American Express* and *Microsoft,* according to a recent report by the US Anti-Phishing Working Group.

The number of phishing scams have increased sharply, according to figures compiled by the UK e-mail security company, *MessageLabs*. In September 2003, they intercepted 279 suspect e-mails. By January 2004 it intercepted 337,350 phishing-related messages. The number intercepted in March 2004 decreased to 215,643 (Bowcott, 2004b). These phishing surges have also been reported by the Association of Payment and Clearing Services.

Combating the fraud has become a priority for the police's NHCTU. Several teams of detectives are investigating but no one has been charged here or abroad. Access to online identities through personal information and passwords appears to be the new easy target. Furthermore, the British economy loses millions of pounds a year as a result of identity fraud. This will only increase if people do not become more aware of their responsibilities to protect their virtual identities. So how can someone protect themselves from the scams?

Anti-spam software

Sometimes, anti-spam software flags questionable e-mail although the method is not failsafe. For instance, some software programs analyse the disparity between good and bad links within a single message, domain and header

* Psychology Division, Nottingham Trent University.

information and looks for a pattern of deception that often results in scare tactics (eg, "your account has been broken into by foreign thieves"). Suspect mail is dispatched to a designated fraud folder.

Common sense
Misspellings, rotten grammar and repeated words in the same sentence are a likely sign a message supposedly from a *bona fide* organization is anything but. (The fake *Barclays* e-mail above is a good example).

Requests for reconfirmation
Requests by a company to have account holders reconfirm personal data that has been lost is a sure sign that the e-mail is a scam. No reputable company asks for passwords and account details in such a manner.

Generic e-mails
Reputable companies will usually correspond with an account holder by their first and last name and/or business affiliation rather than "Dear Lloyds TSB Bank Customer".

Attachments
As with any e-mail, be wary of attachments. Fraudsters have sent mail pretending to be security bulletins, only it was a virus.

References

Bowcott, O. (2004a) "Who's logging in to your account?" *The Guardian,* April 17, p.3.
Bowcott, O. (2004b) "Online accounts face massive rise in "phishing' scams." *The Guardian,* April 17, p.1.
Cowan, R. (2004) "Cyber-crime costs business billions." *The Guardian,* February 25, p.11.
O'Hara, M. (2004) "Identity theft soars." *The Guardian (Jobs and Money),* March 13, p.7.