South African Journal
of Information Management
[DoE accredited]

Peer Reviewed Article Vol.7(3) September 2005

Investigation of phishing to develop guidelines to protect the Internet consumer's identity against attacks by phishers

R. Butler
Department of Accountancy
University of Stellenbosch
Stellenbosch
South Africa
rbutler@sun.ac.za

Contents

Key words: Phishing, password harvesting fishing, identity theft, disclosure of personal information

1 Introduction

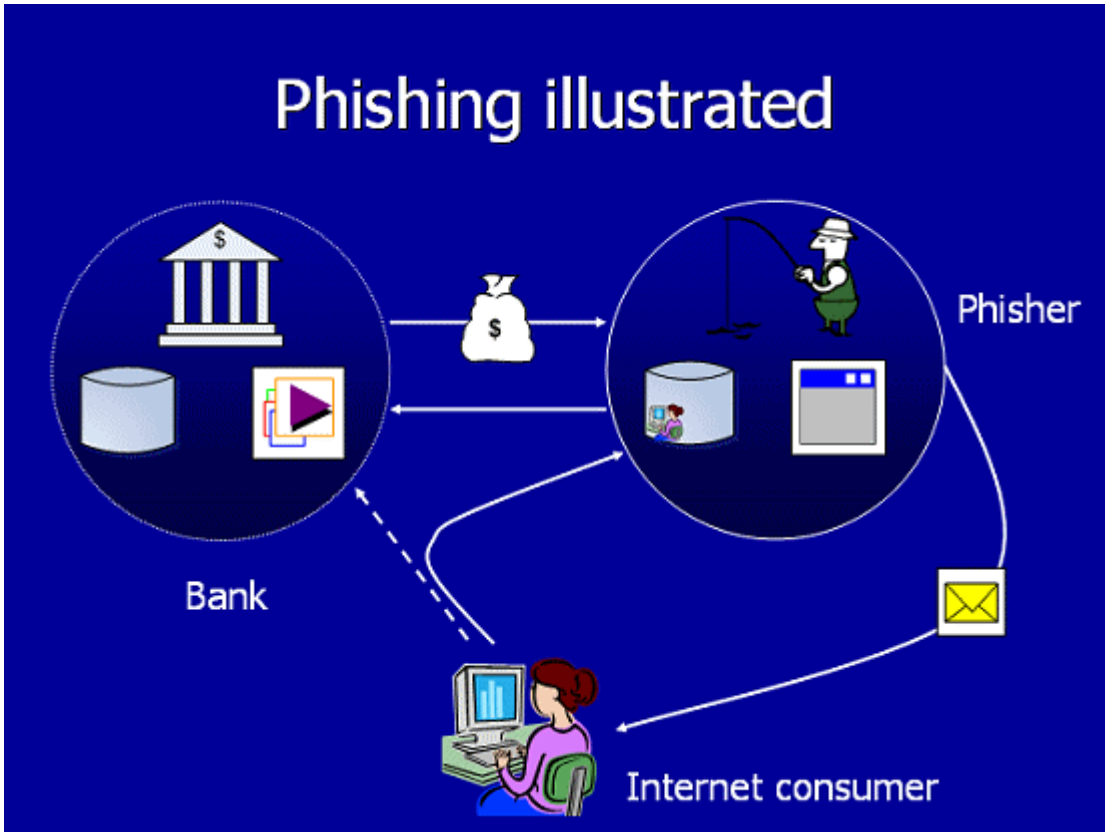
As widely publicized in the local media (*Business Times* 2005; Independent Online 2005; *Mail & Guardian* 2005), the first phishing scam imitating South African banks hit South Africa in May 2005 (Cobbett 2005; Vegter 2005a). Bank clients countrywide received e-mails purporting to come from local banks, requesting them to verify their personal account information. In response to the scam, all four of the major South African banks posted warnings regarding phishing on their Web sites during the same month (Cobbett 2005).

A White Paper on phishing explains that the word *phishing* originates in the term 'password harvesting fishing' (Honeynet Project and Research Alliance 2005). The Anti-Phishing Working Group (APWG), an industry association focused on eliminating identity theft and fraud that results from the growing phishing problem, describes phishing as a process using spoofed e-mails, designed to lure recipients to Web sites, where phishers attempt to trick consumers into divulging personal financial information, such as passwords and account numbers, in order to commit fraud (Anti-Phishing Working Group 2005).

In the often anonymous world of e-commerce, key factors such as passwords and account numbers identify consumers uniquely, in such a way that the Internet user can interact with others and conduct transactions via the Internet. Phishing is an online method that identity thieves can use to obtain the particular sensitive personal information necessary to commit identity theft.

According to Roland le Sueur, head of Internet banking at First National Bank, the primary objective of phishing is to obtain money fraudulently from customers (Vegter 2005a). A phisher uses a stolen identity to contact the organization concerned, claiming to be the victim of the phishing attack, in order to illegally transact business with the organization, in the name of the client concerned. Successful phishing of identities therefore leads to significant financial costs and losses for the victims. Identity theft cost Americans $52,6 billion in 2004 alone (Reuters 2005b).

Figure 1 Graphical presentation of a typical phishing attack



top

2 Extent of the phishing problem

Researchers agree that the first phishing attacks were launched in late 2003 (ActivCard 2004). Since then, the phishing problem has grown significantly and, according to security researchers, this type of scam is currently one of the most prevalent Internet threats (Pruitt 2005). The Denver-based First Data Group, one of the largest electronic financial transaction companies in the USA, recently released telephonic survey results that Synovate conducted with 2000 participants, showing that 43% of USA adults have been subjected to phishing (Tsai 2005).

At the beginning of 2004, the APWG reported that most of the major banks in the USA, United Kingdom and Australia had been misrepresented by phishers. By the end of December 2004, Symantec was seeing an average of 33 million phishing attempts per week, up from an average of 9 million per week in July 2004 (Clarkson 2005b). At the end of 2004, phishing attacks had reached 57 million US adults and had compromised at least 122 well-known brands (Reuters 2005a).

Research indicates that between 3% and 5% of the adults targeted unwittingly provide personal information to phishers (Goldsborough 2004; Tsai 2005). Similar research into fraud-related practices, performed by Gartner in April 2004, indicated the strong correlation between people who recall providing personal information in response to what, in retrospect, was a 'phish mail' and those who suffered identity theft (Bielski 2004; Litan 2004a). According to the results of the survey, a respondent to a phishing e-mail message is three times more likely to experience negative consequences associated with identity theft. The information sought by phishers can also be sold to and bought from identity theft rings (ABSA 2005; Hubbard 2005), thereby increasing the number of possible sources from which phishers can launch their attacks.

At the end of 2004, Patrick Evans, Symantec Africa's regional manager, predicted that phishing was likely to continue to be a critical source of concern during 2005 (Clarkson 2005b). His prediction came true as all four of the major South African banks did indeed become targets of phishing attacks towards the end of May 2005 (Cobbett 2005).

According to the Phishing Activity Trends Report of the APWG, the number of monthly phishing attacks has grown so much during recent months that it has reached epidemic proportions. During May 2005, victims reported 14987 phishing scheme e-mails to the APWG, an increase of approximately 214% over the monthly number of reports received just seven months ago in October 2004. In the same month 3326 phishing sites were active, a 291% increase over the 1142 sites reported in October 2004. Roland le Sueur declares that he thinks phishing currently provides one of the leading fraud risks (Vegter 2005a), a risk that the FBI regards as the 'hottest and most troublesome' scam on the Internet (ActivCard 2004).

Visit the APWG's Web site at http://www.antiphishing.org for the latest monthly Phishing Activity Trends Report.

top

3 Cause of the problem

Brett Myroff, CEO of Sophos distributor Netxactics, states that humans are 'the weak link in the security chain' (Clarkson 2005a). Researchers from the Honeynet Project and Research Alliance, which focuses on collecting data gathered from observing real-world incidents, has concluded that launching phishing attacks on home or small business computers appears to be particularly popular, presumably because 'the systems are often less well managed'. Lack of sound security practices by individuals provides fraudsters with a base from which to launch phishing attacks on unsuspecting consumers (Honeynet Project and Research Alliance 2005).

British research conducted for the 2005 Infosecurity Europe event revealed that an alarming nine out of ten individuals leave themselves vulnerable to identity theft. More than 180 of the 200 respondents questioned freely divulged personal information that fraudsters could use to commit identity theft (Clarkson 2005a).

top

4 Possible solution

As phishers rely on their ability to trick unskilled consumers (Honeynet Project and Research Alliance 2005), Internet consumers need to address the problem by consciously striving to become more aware of the risks of providing sensitive data online; by adopting improved security practices (Clarkson 2005a); and, according to Gartner, by continually updating their knowledge regarding such risks by benefiting from relevant educational programmes (ActivCard 2004; Swann 2005).

Internet consumers need to be informed about the threats posed by phishers, to enable them to protect their identities adequately against identity theft. Internet consumers need to know of the possible risk of identity theft; they need to be familiar with the tell-tale signs of a typical phishing attack; and, more importantly, they need to know how to prevent such attacks, as well as how to react appropriately and promptly on discovering that they have already fallen prey to a phishing attack.

top

5 Objective and research methodology

Even though there are various ways in which identity thieves can steal identities offline (such as by stealing records from businesses or institutions; by bribing employees; by stealing mail, including bank and credit card statements; or by obtaining personal details for fraudulent ends from carelessly discarded credit card or automatic teller machine transaction records), this research only investigated one method of online identity theft, namely phishing.

In this article, the author discusses the *modus operandi* of phishers, as well as the possible results of successful phishing attacks. After a literature review of the relevant available sources, the basic components of a typical phishing scheme, including the phishing message itself, are analysed.

Based on the investigation performed, the article provides guidelines for actions that Internet consumers can take to prevent, detect and recover from phishing attacks. By applying the precautionary and remedial actions proposed in this article, an Internet consumer should be able to prevent falling victim to a successful phishing attack and should also be able to counteract the negative consequences of a phishing attack to which he or she has fallen prey.

top

6 Phishing scheme components

A phishing attack consists of three distinct parts: the e-mail message; a fraudulent Web site; and a hyperlink that leads to the fraudulent Web site, details of which are embedded in the e-mail message concerned (Honeynet Project and Research Alliance 2005; Mogull 2004).

- The **e-mail message**, appearing to come from a legitimate source, is carefully designed to trick the recipient into providing sensitive personal information, which the phisher uses in a fraudulent manner. The message usually contains a section (the 'bait') that requests the user's assistance in solving a problem. (For more details about the phishing message, see the next section of this article, which discusses this aspect in greater depth.)
- The **fraudulent Web site** that the phishers set up mimics the graphics and formatting of a legitimate Web site as closely as possible, in order to mislead the victim deliberately. Well-known online brands are often targeted in this way. The APWG reported that 107 brands were hijacked by phishing schemes in May 2005 – a 135% increase from April 2005 (Anti-Phishing Working Group 2005). On the Web site the user is prompted to provide confidential personal information that the phisher harvests for his or her nefarious ends.
- The fraudulent Web site's name is hidden in an **embedded hyperlink** in an HTML-formatted e-mail, in order to disguise the address of the actual Web site the user will be taken to when clicking on the hyperlink.

This article does not include a technical description of what happens during a phishing attack. The reader can visit http://www.honeynet.org/papers/phishing for a more technical description of the actual techniques and tools used by phishers.

top

7 Successful communication of the phishing message

Successful communication of the phishing message relies on three main aspects: the sender,

the recipient and the content of the phishing e-mail.

7.1 Sender

Phishers typically pose as figures of authority such as banks, credit card companies and other institutions that are in authori z ed possession of sensitive personal information relating to their clients. The fraudsters send out e-mail messages to potential victims, falsely claiming to be from the legitimate organizations concerned. The online thieves rely heavily on the victims' innate sense of truthfulness when responding to automated systems or to (apparent) authority figures (Honeynet Project and Research Alliance 2005). The April 2005 Phishing Activity Trends Report of the APWG indicates that 84% of the 11 new brands hijacked in April 2005 originated in the financial services industry (Anti-Phishing Working Group 2005).

7.2 Recipient

To reach the maximum number of potential victims while subjecting themselves to minimal risk, phishers found 'an ideal partner in crime in the form of spam e-mail' (Honeynet Project and Research Alliance 2005). Spam consists of unsolicited commercial e-mail, usually sent from hacked machines (Bellovin 2004). Patrick Evans reports that up to 73% of the mail traffic of a number of South African corporate environments monitored is spam-related and, thus, susceptible to phishing attacks (Clarkson 2005b).

Legitimate addresses required to create spam can be purchased by thieves on the 'cyber black market', or parsed together using programs that randomly combine last names and first initials with common domain names (Bielski 2004). The senders of bulk phishing messages know that the vast majority of the people to whom they send such messages will simply disregard the messages, as they ordinarily have no dealings with the organization named in the e-mail. However, they are also aware of the fact that a small percentage of the recipients of the mail messages might be account-holders of the targeted organization and respond to the e-mail as though it were authentic, thus making it worthwhile for the attackers to continue their practice (Sophos 2005).

7.3 Content of the phishing e-mail message

Both in terms of the 'look' of the message and the code used, phishers are able to mimic authentic messages emanating from the organizations concerned more and more closely (Bielski 2004). The e-mails sent out by phishers, purporting to be from the organizations themselves, may even feature corporate logos and formats similar to those used by the legitimate organizations.

The e-mail messages usually lure recipients to malicious Web sites, where the victims are duped into disclosing personal details, by means of apparently innocent requests, such as requests for the assistance of the client in solving a 'problem' with his or her account, managing or updating customer information, or requests for urgent action by the user, often, ironically, 'to protect the user's confidential data from malicious activities' (Honeynet Project and Research Alliance 2005). The e-mail recipient may be warned that if he or she fails to respond promptly, a penalty, such as the closure of his or her account, will be imposed.

E xamples of phishing attacks that have been reported to the APWG can be found at http://www.antiphishing.org/phishing_archive.html.

8 Results of phishing as a method of identity theft

Research by Gartner shows that phishing victims are likely to suffer identity theft fraud (Litan 2004a). Identities stolen online can result in the loss of funds and new account fraud (all the figures reported in this section relate to the period 1 May 2003 to 30 April 2004) (Litan 2004b):

- *Illegal purchases* made with the stolen account information are the most common type of fraud committed with stolen identities. Such purchases have resulted in more than $4,5 billion worth of direct losses among approximately 5,7 million online US adults (4% of the online US population).
- *Unauthorized transfers, withdrawals and cash advances* from accounts of which information was obtained have resulted in nearly 2 million online consumers suffering annual losses amounting to nearly $2,4 billion in unauthorized transfers from their accounts. Illegal credit card cash advances have resulted in $1 billion losses and have affected more than 500000 online customers.
- Identity thieves can open new accounts or obtain credit in the victim's name to make *unauthorized purchases* of which the victim is unaware. It is estimated that this type of fraud affected 1,2 million online US adults, resulting in damages amounting to $2,3 billion for online US adults.

To prolong the period before the fraud is discovered, the thieves often change the billing addresses on the accounts targeted.

Other consequences of successful phishing include the following:

- Victims may be refused loans, education, housing and cars, due to bad credit reports. According to the Federal Trade Commission (FTC), victims of identity theft could spend several months, or even years, and vast amounts of money in recovering their good names and credit records (FTC 2005b), after they were damaged by identity thieves.
- Victims usually experience a number of negative emotions, ranging from humiliation to anger and frustration (FTC 2005b).
- Phishing can cause consumers to lose confidence in the e-commerce industry (Litan 2004a). According to a White Paper drafted by ActivCard, phishing attacks the basic element of trust essential for ongoing e-commerce (ActivCard 2004). Brad Nightengale, the vice-president of Visa, states that consumers perceive the online environment as 'exceedingly risky' and that this perception 'could curb online spending' (Radcliff 2005b).

These concerns are supported by a variety of studies. According to Cyota, a fraud prevention service provider, more than 50% of Internet consumers are afraid to conduct online commerce, due to phishing concerns. A Symantec study shows that nearly one-third of the respondents refrain from online banking, due to fears of phishing. Seventy per cent of the Cyota survey participants said that they were less likely to respond to an e-mail purporting to come from a bank, because of fears relating to phishing (Radcliff 2005b).

Internet analysts fear that the phishing threat will slow down, and possibly totally erode, online commerce. Gartner warns that US e-commerce may slow to 10% or less by 2007 (in contrast to the 20% or more annual growth rates experienced in the past), if these concerns are not adequately addressed (ActivCard 2004).

top

9 Combating phishing

Based on the information gathered in this research, the aspects and precautionary measures below should be borne in mind by Internet consumers while interacting on the Internet. By doing so, a consumer will reduce his or her risk of falling victim to a successful phishing attack.

9.1 Aspects and precautionary measures aimed at addressing phishing

Be cautious with e-mails and confidential information.

- E-mail is a relatively insecure means of transmitting financial and personal information. Legitimate companies usually refrain from asking clients to supply sensitive personal details via e-mail.
- Personal e-mails from legitimate companies should be addressed to the consumer directly. A message addressed to 'Dear valued customer' indicates that the message was sent out in bulk, thus rendering it more susceptible to phishing. Consumers should never provide personal information to such requests.
- If the consumer is suspicious about an e-mail message received, he or she should phone the institution that supposedly sent the message, in order to confirm and verify the origin of the message. The official call centre number of the institution concerned should be contacted and not the one provided in the e-mail message concerned.
- The consumer must check the messages received for spelling mistakes and bad grammar. Grammatically incorrect or misspelt messages may indicate irregularities. Official communications are usually checked for language proficiency before being sent out.
- The consumer must check that e-mail messages requesting personal details are signed by an official of the company concerned.

Examine the URL (Uniform Resource Locator) displayed in the address or status bar at the bottom of the browser frame.

The link to a Web site to which an e-mail refers recipients can be disguised in various ways. Standard HTML code can be used to provide misleading information (Sophos 2005). The APWG reported that 46% of the May 2005 phishing attacks contained some form of the target name in the URL (Anti-Phishing Working Group 2005).

- Only a certain number of characters of the URL can be displayed. The longer the URL, the easier it is for the identity thieves to conceal the true destination the Internet consumer will be taken to when activating the link. Phishers can place the 'active' part of the URL at the end of the string, obscuring it from view (Sophos 2005).

  Note that most browsers ignore characters preceding the @ symbol in a URL. For example, http://www.legitimatecompany.com@phishingscam.com will actually take the user to Phishingscam.com's site, and not to the Web page of Legitimate Company.

  The true URL might be disguised by the substitution of similar-looking characters in the URL. At first glance, the URL might appear to be the name of the organization the Internet consumer is familiar with. However, the name might have been slightly altered by means of the intentional addition, omission or transposition of letters, or by means of the addition of certain hyphens or dots.

  One of the first phishing incidents reported disguised Paypal.com as paypa1.com

(Bellovin 2004). Similarly, the Web site address www.microsoft.com could appear as www.micosoft.com, www.microsift.com or www.verify-microsoft.com (Microsoft.com 2005).

The user should not cut and paste the link provided in an e-mail message. He or she should retype the URL directly into the browser rather than click on hyperlinks contained in e-mails. Typing in the URL will take the user directly to the relevant Web site. (Alternatively, the user can add the institution's address to his or her list of favourite Web sites, and use this link whenever he or she wants to log onto the relevant Web site.)

- Look for indications that the browser and Web site are secure and legitimate.

  Ensure that the Web site address is prefixed with 'https' (the 's' is for secure) and not just 'http'. A picture of a padlock (locked symbol) appears on the bottom right of the browser page or status bar in Internet Explorer, indicating a secure Web site. (If there is no status bar at the bottom of the browser window, click on 'View' at the top of ther browser and then select 'Status bar' to activate it.) The closed lock must be present on all pages requesting personal information.

  Unfortunately, no indicator is totally foolproof, as phishers can even forge security icons. The consumer must verify that he or she is visiting a secure Web site by checking the security certificate of the site concerned. He or she should double-click on the lock icon to display the security certificate. The name following 'Issued to' should match the name of the legitimate site the consumer intended to visit.

- The consumer should look for the Web site's privacy policy, which describes how the personal information a site collects will be used and protected. If the privacy policy is not displayed or the user is unable to understand it, he or she should consider doing business elsewhere.

Only donate funds online through the Web sites of designated fund-collecting organizations which are government-registered and which have NPO numbers. Such organizations are registered in terms of the *Non-Profit Organizations Act, No 71 of 1997*, and usually have secure online payments sites.

Phishers may launch attacks in which they play on people's emotions. For example, in the aftermath of the tsunami disaster of December 2004, phishers took advantage of the outpouring of goodwill, and the subsequent call for donations, by setting up false Web sites on which they claimed to be raising funds for disaster relief and offering to locate missing people. Ann Bown, external relations officer for the South African Red Cross Society, estimates that between 5% and 10% of funds raised for charity or disaster relief efforts are skimmed by scam artists (Vecchiatto 2005).

Consumers should treat supposed 'bargains' (which could be examples of 'google phishing', as described later in this article) advertised on Web sites with suspicion and only buy from trusted sites, as described above. He or she should bear in mind that, if an offer appears too good to be true, it most probably is.

Consumers should regularly check the activity on their accounts and review credit card and bank statements for unauthorized charges as soon as they are received. If a statement is more than a couple of days late, the consumer should call the bank to confirm the billing address and account balance, as identity thieves often change billing addresses to delay detection of

any fraudulent transactions.

9.2 Other general security measures

The following general security measures might also assist in providing a safe environment and in minimizing the risk of a successful phishing attack.

- Be suspicious of e-mails arriving from unknown sources.
- Delete all suspicious e-mails immediately.
- Use up-to-date spam filter and anti-virus software, in order to reduce the number of fraudulent and malicious e-mails to which you might otherwise be exposed.
- Install firewalls to block uninvited access to your computer.
- Install the patches that software providers distribute to close holes hackers or phishers might otherwise exploit.
- Apply sound password control on all accounts and computers.
- Delete all personal information on computers that are disposed of.
- Activate and use the SMS security feature and the random verification number as a prerequisite for beneficiary creation when using Internet banking. The consumer will then be notified via SMS of any activity on his or her bank account.
- Stay informed about the latest news on fraudulent Internet activity.

Immediately report any suspicious activity or e-mail received directly to the faked or 'spoofed' organization (by, for example, calling the customer services toll-free number, and not the number provided in the e-mail message) and to the relevant authorities, including the South African Fraud Prevention Service (which can be reached at 0860101248) and the APWG (http://www.antiphishing.org).

top

10 What to do if a person finds that he or she has provided personal information to a phisher

If a consumer finds that he or she has provided personal information to a phisher, the following guidelines will minimize potential loss.

- Change the passwords on all accounts as soon as possible.
- Review credit card and bank statements closely in order to detect possible unauthorized activity.
- Immediately, in writing, close the accounts that are known or suspected to have been tampered with.
- Report the incident to the credit card company concerned; the company that has been fraudulently misrepresented; the South African Fraud Prevention Service and the APWG.
- Request that the fraud departments of the local credit bureaus place a fraud alert on the credit file or report. Check and monitor one's own credit report.
- File a report of the incident at the local police station. Secure a copy of the report, or at least the case number concerned, to provide proof of the crime to creditors who may need it.
- Invest in an anti-spam filter and in anti-virus software to filter the messages received in future.

top

11 After a phishing attack is reported

The good news is that the reported phishing incidents are investigated by the relevant authorities, who question the alleged phishers. The phishing Web sites that are discovered are then shut down and the perpetrators arrested.

A number of people allegedly involved in the recent South African phishing attacks were questioned by the Investigation Unit of the Scorpions to help the police uncover possible international syndicates (Lowman 2005). According to Hemmanth Singh, director of technology engineering at the Standard Bank, the Internet service providers co-operate in taking sites offline if evidence of illegal activities are provided (Vegter 2005b). The Phishing Activity Trends Report of the APWG states that the average time online for a phishing site during May 2005 was 5.8 days, the longest time was 30 days (Anti-Phishing Working Group 2005), before being shut down.

top

12 Phishing without a lure

The bad news is that due to ongoing innovations and advancements in the 'art of phishing', new phishing techniques are already, no doubt, under development (Honeynet Project and Research Alliance 2005). Although this research is an attempt to cover the field as it currently stands, it might, therefore, not cover all possible phishing methods and techniques.

According to the APWG, phishers are learning how to avoid the signs of conventional phishing techniques (Anti-Phishing Working Group 2005).

These new phishing 'mutations' include 'pharming', 'spear fishing' (keylogging), 'google phishing' and 'wi-phishing' (Jones 2005; Radcliff 2005b).

- **Pharming (or DNS poisoning)** involves redirecting unsuspecting Internet users to counterfeit (phish or password-harvesting) sites that closely resemble the legitimate site, when a legitimate domain's name is entered. Pharmers inject malicious code onto a PC, or even onto DNS servers on the Internet. When logging on to the counterfeit site, the personal information used for logging on is harvested and transmitted to the pharmers concerned (Anti-Phishing Working Group 2005; Fox 2005; Hubbard 2005; Radcliff 2005b).
- In **spear fishing (or keylogging),** fraudsters load programs, known as keystroke-loggers, onto the end user's directory. Upon rebooting the computer, the application modifies the system registry files and tracks the keystrokes of people using infected machines. The keystroke-loggers activate when certain keywords are typed into browsers, or when specific predetermined sites are accessed (Der Hovanesian 2005; Gilbert 2005; Radcliff 2005a; Radcliff 2005b).

  For example, the keystroke-loggers can capture the login names and passwords for online bank accounts when customers do e-banking and send this personal information to the attackers. Keystroke-loggers can become hidden and infect computers in various ways, including the opening of phony e-mail attachments, on downloading programs online (usually 'free' software), and through fraudulent Web sites, accessed when users mistype the names of common Web sites (Der Hovanesian 2005; Gilbert 2005; Radcliff 2005a; Radcliff 2005b).

  The March 2005 Phishing Activity Trends Report of the APWG reported a dramatic increase in the amount of phishing-based malicious code designed for logging keystrokes. From February to March 2005, researchers reported discovering eight to ten new keylogging systems and more than 100 crimeware

hosting Web sites per week, in comparison to the discovery of an average of one to two new phishing keylogger variants and ten to 15 new malicious Web sites hosting this code per week from November 2004 through to December 2004 (Anti-Phishing Working Group 2005).

- In **google phishing**, phishers use search engines to drive traffic to illegitimate sites, on which they claim to be selling a product or service, usually at unbelievably low prices. The phishers set up fraudulent Web sites and, as they have no intention of making any legitimate sales, they can claim to be selling virtually anything at any price that they think is likely to attract victims to their Web site. With this form of attack, phishers do not initiate contact with their potential victims, but the Internet consumers themselves search out the phishing site by means of entering certain key terms in a search engine, such as when, for example, searching for the cheapest online airline tickets. Internet consumers, having appeared to have 'found' the site by themselves, gain a false impression of it being a secure and legitimate site (Radcliff 2005b).

  When buying from the site, users have to complete forms requiring their personal details, including their credit card information and expiry dates, online. On submission of the form, an error message is displayed, informing the consumer that a problem had occurred and that the transaction was not completed successfully. Meanwhile, the phisher will already have gained access to the information concerned, which may be used for future fraudulent purposes (Corrons 2005; Radcliff 2005b).

- **Wi-phishing** entails the phishing of personal information from consumers who make use of wireless technology and Bluetooth facilities. The cybercrooks set up wi-fi networks in public places, which users of wireless broadband connections tend to frequent. While using what they might assume are legitimate networks at designated hotspots, the users can have their personal information (in the form of keystrokes and passwords) tapped into by wi-phishers, who harvest personal information through their own networks (Der Hovanesian 2005; Radcliff 2005b).

top

13 Conclusion

For most purposes, an online consumer is only a number transacting over the Internet. The Internet consumer should actively protect the confidentiality of his or her online identity in order to prevent identity theft. Online consumers need to learn how to prevent and cope with fraudulent Internet activity aimed at extracting personal details for the financial benefit of phishers. A consumer should be able to recognize the signs of a possible phishing attack and know how to react to a phishing e-mail message that he or she receives.

By considering the various aspects covered, and by applying the precautionary measures suggested in this article, the Internet consumer will significantly reduce his or her chances of falling prey to phishing attacks. The actions recommended in this article to Internet consumers who have responded to phishing messages, should also assist in minimizing the negative effects that might otherwise be suffered as a result of phishing. Al DiGuido, CEO of Bigfoot Interactive, asserts, in an article named 'Study: Fraud is Consumers' No. 1 Concern', '[p]hishing will only be diminished when people are completely educated' (Oser 2005).

top

14 References

ABSA. 2005. *Online Fraud Update.* [Online]. Available: http://www.absa.co.za [Accessed 8 June 2005].

ActivCard. 2004. How to catch a phish. *White Paper*. [Online]. Available: http://www.activecard.com [Accessed 8 June 2005].

Anti-Phishing Working Group (APWG). 2005. *Phishing activity trends report.* [Online]. Available: http://www. antiphishing.org [Accessed 19 July 2005].

Bellovin, S.M. 2004. Spamming, phishing, authentication, and privacy. *Communications of the ACM* 47(12). [Online]. Available: http://www.proquest.umi.com [Accessed 8 June 2005].

Bielski, L. 2004. Phishing phace-off. *ABA Banking Journal* 96(9):46. [Online]. Available: http://www.proquest.umi.com [Accessed 8 June 2005].

Business Times . 2005. ABSA falls victim to net scam. [Online]. 19 May 2005. Available: http://www.finance24.com [Accessed 25 May 2005]

Clarkson, D. 2005a. *Humans still the weak security link.* [Online]. Available: http://www.itweb.co.za [Accessed 20 May 2005].

Clarkson, D. 2005b. *Wanted: your personal info.* [Online]. Available: http://www.itweb.co.za [Accessed 20 May 2005].

Cobbett, J. 2005. *Phishing spree.* [Online]. Available: http://www.moneyweb.co.za [Accessed 25 May 2005].

Corrons, L. 2005. Phishing scam twist: bogus sites built to snatch credit cards. *TechWeb.* [Online]. Available: http://www.proquest.umi.com [Accessed 23 May 2005].

Der Hovanesian, M. 2005. Hackers and phishers and fraud, oh my! *Business Week* (3935):81. [Online]. Available: http://www.web20.epnet.com [Accessed 8 June 2005].

Federal Trade Commission (FTC). 2005a. *How not to get hooked by a 'phishing' scam.* [Online]. Available: http://www.ftc.gov [Accessed 20 May 2005].

Federal Trade Commission (FTC). 2005b. *Take charge: fighting back against identity theft.* [Online]. Available: http://www.comsumer/gov/idtheft [Accessed 20 May 2005].

Fox, S. 2005. Here comes phishing on steriods. *Plugged in* 23(6):32. [Online]. Available: http://www.pcworld.com [Accessed 8 June 2005].

Gilbert, A. 2005. *Phishing attacks take a new twist.* [Online]. Available: http://www.news.com [Accessed 20 May 2005].

Goldsborough, R. 2004. Don't get 'phished' out of cyberspace. *Black Issues in Higher Education* 21(21):37. [Online]. Available: http://www.proquest.umi.com [Accessed 8 June 2005].

Honeynet Project and Research Alliance. 2005. Know your enemy: phishing – behind the scenes of phishing attacks. *White Paper.* [Online]. Available: http://www.honeynet.org/papers/phishing [Accessed 23 May 2005].

Hubbard, D. 2005. Phishers moving away from e-mail 'lures'. *Techweb.* [Online]. Available: http://www.proquest.umi.com [Accessed 23 May 2005].

Independent Online. 2005. Offshore phishing scam hits SA banks. *The Star* 20 May. [Online]. Available: http://www.iol.co.za [Accessed 20 May 2005].

Jones, K. 2005. Pharming your identity. *PC Magazine* 24(8). [Online]. Available: http://www.web33.epnet.com [Accessed 23 May 2005].

Litan, A. 2004a. *Phishing victims likely will suffer identity theft fraud.* [Online]. Available: http://www.gartner.com [Accessed 8 June 2005].

Litan, A. 2004b. *US consumer fraud spreads its tentacles across channels.* [Online]. Available: http://www.gartner.com [Accessed 8 June 2005].

Lowman, S. 2005. *Phishing suspects questioned.* [Online]. Available: http://www.itweb.co.za [Accessed 8 June 2005].

Mail & Guardian. 2005. ABSA also targeted in e-mail scam. 10 May. [Online]. Available: http://www.mg.co.za [Accessed 25 May 2005].

Microsoft.com. 2005. *Help prevent identity theft from phishing scams.* [Online]. Available: http://www.microsoft.com [Accessed 20 May 2005].

Mogull, R. 2004. *How to spot, and stop, 'phishing' e-mail attacks.* [Online]. Available: http://www.gartner.com [Accessed 8 June 2005].

Oser, K. 2005. Study: fraud is consumers' no. 1 concern. *Advertising Age* 76(13). [Online]. Available: http://www.web33.epnet.com [Accessed 23 May 2005].

Pruitt, S. 2005. Firefox users snap up anti-phishing toolbar. *Network World* 22(21):20. [Online]. Available: http://www.networkworld.com [Accessed 8 June 2005].

Radcliff, D. 2005a. Phishers use spears, hooks and nets. *Network World* 22(12):20. [Online]. Available: http://www.proquest.umi.com [Accessed 23 May 2005].

Radcliff, D. 2005b. Fighting back against phishing. *Network World* 22(14):48. [Online]. Available: http://www.proquest.umi.com [Accessed 23 May 2005].

Reuters. 2005a. Internet phishing scams getting more devious. [Online]. Available: http://www.itweb.co.za [Accessed 20 May 2005].

Reuters. 2005b. More identity theft offline than online. [Online]. Available: http://www.itweb.co.za [Accessed 20 May 2005].

Sophos. 2005. Phishing and the threat to corporate networks. *White Paper* May 2005. [Online]. Available: http://www.sophos.com [Accessed 8 June 2005].

Swann, J. 2005. Anti-phishing group reports that phishing attacks still on the rise. *Wireless News* 30 April. [Online]. Available: http://www.web33.epnet.com [Accessed 23 May 2005].

Tsai, C. 2005. *Survey: 43 percent of adults get 'phished*'. [Online]. Available: http://www.siliconvalley.com [Accessed 20 May 2005].

Vecchiatto, P. 2005. *Web scammers cash in on tsunami.* [Online]. Available: http://www.itweb.co.za [Accessed 20 May 2005].

Vegter, I. 2005a. Plugging the 'phishing' hole. *iWeek,* 5:16-18.

Vegter, I. 2005b. Not just a phishing expedition. *Brainstorm:* 8-9.

ISSN 1560-683X

Published by InterWord Communications for Department of Information and Knowledge Management, University of Johannesburg