Phishing: A Growing Challenge for Internet Banking Providers in Malaysia

Gerald Goh Guan Gan, Tan Nya Ling, Goh Choon Yih & Uchenna Cyril Eze
Knowledge Management Group, Multimedia University, Melaka, Malaysia

Abstract

Internet banking in Malaysia has the potential to develop further into a key e-service application that is beneficial to both Internet banking providers and users. To achieve this, a critical mass of Internet banking users needs to be developed and sustained. However, there is growing concern over the erosion of user trust towards this alternative banking channel, stemming from the rise in identity theft cases in the past few years. Phishing is becoming a major problem for users and is creating an ever-greater issue for Internet banking providers who need to find ways to mitigate the effects of phishing to their operations. This paper outlines the modus operandi of a typical phishing attack and provides a brief overview of the different types of phishing. It is evident that everyone needs to play an active role in addressing this with governments and crime prevention authorities having to come up with the necessary legislation and measures to protect all stakeholders in the Internet banking arena. In addition to that, Internet banking providers need to come up with adequate security systems to minimize the phishing threat to users. More importantly, users need to be educated and made aware of the problem through effective education and awareness programmes. This paper identifies some measures and issues that would require the attention of anti-phishing educators to ensure the effectiveness anti-phishing initiatives.

1. Introduction

Internet banking is a fast growing alternative banking channel in Malaysia and is poised to become the primary channel for banking transactions by the turn of the decade. If compared with other payment channels, the Internet affords many advantages to both banks and customers, especially in terms of its low cost, ease of access in terms of time and space, convenience and user control [1]. Consequently, banks have increased investments in Internet banking services and reduced the number of branch offices and payment automated teller machines (ATMs). This has encouraged better service offerings to a growing customer base with a preference for Internet banking applications.

Despite Internet banking's rapid growth and increased acceptance in Malaysia, local banks are still required to maintain a wide network of physical bank branches and ATMs despite the inherent low cost advantages of Internet banking transactions [1-4]. This is mainly due to the resistance of certain segments of users in adopting Internet banking due to a wide array of issues and barriers which are not sufficiently recognized by industry players [1, 2, 5].

Whilst the literature is flooded with studies on user adoption of technologies such as Internet banking, studies that focus on user resistance or rejection of technological innovations are limited [1, 6]. Majority of the innovation-based studies focused on the successful innovation and diffusion of the innovation among its users. According to Kuisma, Laukkanen and Hiltunen [1], this is mainly due to '…biased idea that all innovations are improvements over existing products providing added value for the majority of consumer [whilst] … resistance to change is seen as a normal consumer response to the changes innovations imply for consumers'. They argue that resistance represents the other side of the phenomenon and there is a need for studies to address both facets of diffusion – adoption and rejection. Sheth [6] asserts that it '…is about time we paid respect to individuals who resist change, understand their psychology of resistance and utilize this knowledge in the development and promotion of innovations rather than thrust upon them preconceived innovations'. One of the key inhibitors of Internet banking is the lack of user trust, which could lead to the escalation of the perceived risk of online banking transactions.

This paper, therefore, examines the key reasons why users would resist Internet banking applications. Suh and Han [7] believe that trust is one of the most important determinants in explaining a user's approach towards using Internet banking. This inhibitor stems from the problem of identity theft in the form of phishing that has grown to become a major issue and a thorn among Internet banking users. Sadly, due to the fast pace of evolution in the technical field, many forms and variants of identity theft mechanisms such as spear phishing, pharming and evil twins have emerged and a brief discussion of these methods ensues. Finally, this paper suggests that technical countermeasures

alone is ineffective in circumventing the phishing menace, instead a comprehensive education and awareness programme should be devised to go hand in hand with other technical countermeasures to minimize the impacts of phishing to the Internet banking sector and regain users trust. The findings presented in this paper is benefits both the industry and users as it provides a comprehensive suggestion of measures that should received more attention by both parties and would allow for the formulation of more effective measures and the adoption of best practices that would enhance the growth of the Internet banking sector.

The following sections provide an overview of phishing and identity theft, a discussion on the *modus operandi* of a typical phishing attack, steps involed in a typical phishing attack and finally some recommendations on ways to combat phishing.

1. Identity theft and the erosion of user trust

Identity theft has existed long before the widespread reach of the Internet in the form of simplistic yet effective techniques of dumpster diving, phone inquisitions and social engineering [8]. However, due to the ubiquitous nature of the Internet these days, identity theft perpetrators are now using the Internet to facilitate their malicious intent [8]. Identity theft is becoming a key concern among Internet banking stakeholders and has been recognized as the most widespread and fastest growing digital crime in the United States of America [9].

Swartz [10], defines identity theft as a 'situation where someone else assumes the identity of another and makes telephone calls or obtains merchandise, credit, or other valuable things in their name'. Identity theft happens as a result of human negligence, physical theft, bugs and malicious software [8, 9]. While many users are still ignorant of precautionary measures to prevent this growing menace, victims of identity theft more often than not would have to spend a considerable sum of money and effort to rectify the problem and may even suffer severe losses if the perpetrators siphoned off funds from their bank accounts undetected [8].

The US Federal Trade Commission estimates that 3.2 million American citizens have their identity stolen, equating to one incident every ten seconds [11]. In Malaysia, the reported incidences of fraudulent computer activity are on a rise as evident from the statistics reported by the Malaysian Computer Emergency Response Team or MyCERT. According to MyCERT [12], there were only 3 reported computer fraud incidences in 2000 but this number rose quickly in the subsequent years to 106 in 2004 and 364 in 2007. Phishing victims reported being deceived into visiting a fake website where perpetrators then stole their usernames and passwords and later used the information for the perpetrators' own advantage [13, 14]. This results in the breach of information security through the compromise of users' confidential data. In light of this, the Association of Banks Malaysia (ABM) has reminded industry players, namely the commercial banks and users to be extra cautious and vigilant when conducting banking transactions online especially with the sharp increase in incidences involving scam emails [13].

Incidences of identity theft have negative repercussions on the adoption [and rejection] of Internet banking, eroding the confidence and trust of users on the system's security and integrity, resulting in growing resistance to the adoption of Internet banking. Foley and Foley [14] broadly categorized identity theft into financial identity theft, criminal identity theft and cloning identity theft. The focus of this paper, however, is the financial identity theft, which is of special interest to Internet banking and occurs when the perpetrator utilizes the victim's identifying personal information to conduct financial transactions [14].

Perpetrators have at their disposal a multitude of methods and tools to steal the identity of unsuspecting victims online. These methods include the use of computer viruses, spyware, Trojans, worms, keyloggers, pharming and phishing [9, 15]. Lately, phishing has gained widespread attention amongst Internet banking industry players and users following numerious reports on online financial identity thefts [16]. Phishing is a fraudulent attempt by Internet criminals to get users to respond to e-mails and websites, thereby unknowingly divulging their personal financial information [15]. Pharming on the other hand is when a 'hacker acquires the Domain Name Server (DNS) or attacks users' browsers to redirect users to a different IP address, where the fake or spoof web site is hosted, with an intention to get users' personal

details'[9]. As such, pharming is said to be phishing without the lure, resulting in a spoofed DNS transporting users who typed a legitimate web address to the 'hijacked' website [17].

2. Phishing *modus operandi*

The term 'phishing' has its origins from the analogy that identity thieves are using lures usually in the form of e-mails to 'fish' for passwords and financial data from the 'sea' of Internet users, coined circa 1996 by hackers who were then stealing America On-Line (AOL) account details by scamming unsuspecting AOL users [17].

Kierkegaard [17] explains that before mid-2003s, most phishing attacks were in the form of text-heavy e-mails, usually embedding web site designs into these e-mails, complete with the logos of the targeted company including return addresses that were spoofed to look as if it came from the company. However, by mid-2004s, perpetrators began to employ the use of novel programming tricks to alter the appearance of the victim's address bar by the replacing the URL of the phishing site with that of the company being impersonated [9, 16, 17]. This proved to be a major breakthrough for identity thieves who are now able to scam millions of users worldwide as it is now difficult to discern between the real and the fake. Gartner Research announced the results of a survey conducted in 2004 showing that an estimated 57 million American adults received e-mail attacks from "phishers". These phishing attacks had somehow undermined user's confidence, which in turn threatened users trust [18].

Classic phishing attack begins when the phisher sends spam to unsuspecting recipients as bait [19, 20]. In most instances, the bait is an e-mail claiming to be from a trusted organization, such as a bank, credit card company or third-party payment organization [9, 21]. The e-mail often claims that the consumer must urgently take action, or else suffer severe repercussions to their interests such as the as the closure of their account [19, 22]. This is demonstrated by a scam email in Figure 1 that claims to have been sent from PayPal requesting users to re-activate their PayPal accounts which have been suspended as a security measure to prevent fraudulent charges from being made to the account.

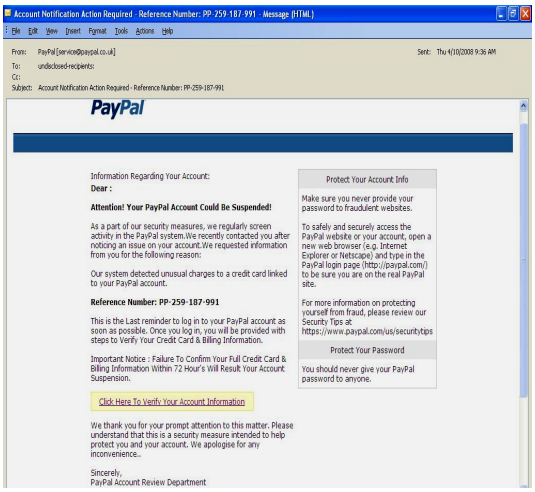

Fig 1. Phishing e-mail claiming to be from PayPal

Once the phisher sends spam with bait, the next step is that the e-mail service provider delivers the bait to the recipients [15, 23]. Next, the recipient will read the e-mail and may end up responding to the scam e-mail by clicking on the spoofed link [16]. The link directs users to a web site that is intentionally designed to look like that of the trusted company i.e. PayPal, Citibank etc but under the control of the phisher [19, 21]. The site would then request the user to enter their personal information such as their account number, password, or identity card number [9]. When the user enters their personal information at a spoofed site, the phishing attack has succeeded its first goal, which is to gather personal information fraudulently [9, 22]. Next, the identity thieves will use the personal information to harm the consumer by hijacking the user's account, credit card fraud, or by using the personal information to purchase goods fraudulently [9, 16, 24]. In short, once the personal information is in the hands of the identity thieves, they would ultimately want to seek to profit from it at the expense of the unfortunate user [22, 25, 26].

A typical phishing attack is usually composed of six sequential stages or phases which are planning the attack, launching the attack, gathering data, determining how to use the gathered data, perpetrate fraudulent activities and launder proceeds obtained [21, 22].

Planning the attack

In the first phase, the computer criminals would strategise and plan an attack to uncover personal information from users [21, 27]. These

perpetrators will normally collaborate and team up with other computer criminals to learn the ropes and eventually mount the attack. Having done that, they will then need to identify and recruit their accomplices [22, 28]. They will have to decide on the intended target/s and decide on what data needs to be gathered from which sources to successfully accomplish their goal [22]. Next, they will decide on the method of attack, which will often be some combination of e-mail phishing, pharming, deceptive downloads, and other available techniques [22]. An entire phishing subculture has arisen, with web sites offering phishing kits that include samples of messages, instructions for building links, and other assistance in preparing and carrying out attacks [9, 17, 22].

Launching the attack

After planning the mechanics of the attacks, the next step is to send out the bait for a phishing attack or find some other way to obtain the users' personal information [22, 27, 28] The best known phishing attack is in the form of an e-mail that asks the consumer for personal information [16, 21]. Other attacks include deceptive downloads onto user computers, pharming attacks and recruiting insiders who can help in harvesting personal information [15, 22, 29].

Gathering data

The working definition of phishing used in this paper is use of the Internet to fraudulently gather personal data about a consumer [15]. Therefore, once the attack has been launched, the criminal needs a way to harvest that personal data [8, 15, 21]. Some of the key methods to gather data include: user entry of data, such as on a spoofed web site or in an e-mail, software capture of data, such as by logging the consumer keystrokes, scraping data from the user's screen or sniffing traffic in the network [17, 21, 22].

Determining how to use the gathered data

Once the criminals have gathered the personal data required, they have to decide how to use it [20, 22]. For attacks against a financial institution or an online merchant, they have to learn the *modus operandi* inherent in the particular transaction — what information is needed for authorization, what credit limits set off alarms, and what kinds of transactions get more scrutiny than others [22, 28]. The criminals also need to select the 'best' customers to attack — those with large assets, good credit limits or other traits that make them a profitable and 'worthwhile' target [22].

Perpetrate fraudulent activities

Next the criminals seek to take advantage of the data they have gathered earlier mainly by making an unauthorized purchase, opening a credit card account under an assumed name or hijacking a bank account and stealing funds from it [14, 22, 27, 28]. The crime may occur on a wholesale basis, such as by selling an entire inventory of credit card numbers or as part of the phishing ecosystem, there are web sites that help phishers fence the personal information of their victims [14, 16, 22]. The crime may be extortion, such as threatening to reveal information or cause other harm unless payment is made [22]. In some instances, the activity may involve terrorism or support for a political agenda, where the gains would be political rather than financial [22, 28].

Launder proceeds

After successfully obtaining money and assets through phishing attacks, the perpetrators need to find a way to launder their ill-gotten gains to avoid detection by the authorities. If they were able to obtain goods or other assets through identity theft, they would then need to convert it into cash and eventually placed into legitimate accounts in legitimate institutions [9, 22, 26]. The nature and characteristics of the Internet and virtual market-space is in fact making it easier for these perpetrators to perform money laundering [24, 25]. 'Furthermore, money is represented by digital bits and other value propositions, thus making it difficult to track and trace'[22, 25]. The exponential growth of these models, particularly those that are non-blank and peer-to-peer, may perpetuate the money-laundering problem by providing technical capabilities to more people and enabling them to operate from the comfort of their own computer terminals [22, 24].

These attacks create a large and growing hazard for many users and other stakeholders as well [30-32]. One obvious hazard to businesses is direct loss, such as when merchants or financial institutions are the victims of fraudulent activity brought about by phishing [26]. The much greater hazard to business, however is the risk of erosion and loss of consumer confidence in Internet banking applications [3, 22]. The decline in user confidence in Internet banking would greatly affect the banks and also the ISPs, software providers, and all other companies

whose business is based on the growth of online activity generally [22, 32]. Internet banking would be greatly affected if users are concerned over the possible presence of malicious software on their computers or if they cannot tell the difference between legitimate banking sites and spoof sites [22].

3. What's next after phishing?

As users are getting more aware of the *modus operandi* of phishing attacks over the Internet, identity thieves are taking measures to deceive the public and to continue harvesting stolen identities online. A variant of phishing that is yielding potent results to these perpetrators is spear-phishing which is more targeted and specific if compared to its predecessor. 'Spear-phishing relies heavily on making the target seem safe to provide believable snare and targets a smaller, more defined groups of victims' [8]. This results in spear-phishing being able to yield better results for identity thieves than conventional phishing attacks. Unlike phishing which sends out the scam to a large pool of 'prospects' which only very few respond, spear-phishing relies on the perpetrators' ability to win the trust of a smaller group of 'prospects', for a long enough time to retrieve the sensitive identification details required [8]. Spear phishing leverages on known institutional affinities of the target group. For example, the perpetrator may comb the web site of an organization for the names and contact details of its employees. It will then send an email to these individuals, purporting to be from the bank, which the organization officially uses for its payroll.

Another growing phenomenon among Internet identity thieves is pharming where perpetrators try to link consumers with their websites and then capture users' personal information [8]. It is important to note that pharming is emerging as a major Internet problem and is expected to 'overtake' phishing as the most dangerous Internet scam tactic [19]. In contrast to phishing that uses e-mail spam to deliver scam e-mails to users, persuading users into revealing their personal information, pharming directs computer users to a phantom website which bears an uncanny similarity to the *bona fide* website [8]. In essence, users are directed to a phantom website that looks the same as the actual site. Most users are not able to tell the difference between this phantom website and the actual site as the address that appears in the web browser will be identical to one that is produced by the actual website. This is accomplished with the alteration of the website address information behind the scenes, thereby perpetuating a phantom website that is an exact replica of the actual site [8]. In essence, pharming is more insidious since users are redirected to a false site without any participation or knowledge on their part [19].

With improved mobility of computers made possible with wireless communication technologies, another method of surreptitiously gathering confidential information from users has emerged. Folsom, Guillory and Boulware [27] explain that a new method termed as 'evil twins' that employs the use of Wi-Fi sites that are created by identity thieves to capture Internet users' personal information when they connect to these staged Wi-Fi sites [8]. These evil twins are Wi-Fi sites that resemble *bona fide* and secure Wi-Fi connections to the Internet. However, these sites have been intentionally set up by the identity thieves to surreptitiously collect personal information of users connected to these sites [8, 27]. In view of the growth of the phishing menace and increase in the number of phishing variants as discussed in this section, it is therefore important for industry players to protect users with the appropriate security features and to provide users with adequate knowledge through continuous education and training to prevent themselves from falling into the phishing trap.

5. Education and awareness: the key to regaining user trust

To mitigate issues brought about by phishing, it is therefore exigent that an appropriate level of education and awareness of the phishing menace among users is achieved. The case for a greater awareness of the issue stems from the large and growing nature of the phishing problem [22]. With the steady increase of phishing attacks over the years and the constantly evolving nature and form of such attacks, Internet banking users face more and more dangerous phishing attacks, posing obvious hazards for the consumers themselves [28]. Governments need to play a central role in addressing this issue by devising guidelines or best practices that should be adhered to by industry players i.e. banks, ISPs and financial firms [33, 34]. Governments should come up with legislation that looks specifically into the issue of phishing and online identity theft. A good example would be the *US Anti Phishing Act 2005* that plays a supporting role in

combating the phishing menace [33]. Before embarking on an aggressive education and awareness programme, Internet banking providers need to come up with phishing-proof mechanisms to ensure the integrity of transactions whilst improving user trust levels.

According to Brody, Mulig and Kimball [34], 'it is likely that over the next several years, banks will spend millions of dollars enhancing information security in response to the recent [US] Federal Financial Institutions Examination Council (FFIEC) guidelines'. The US FFIEC guidelines were updated in response to the increased threats from phishing and pharming scams and recommends that financial institutions assess the risk associated with their Internet banking applications, identify mitigating actions and adjust their information security programs to implement those actions [34]. Interestingly, the US FFIEC does not consider an identification name and password alone as a sufficient security measure for Internet-based banking [34]. Therefore there is a need for additional controls such as multi-factor authentication and mutual authentication to be implemented to deter future fraudulent activity from occurring [34]. Multi-factor authentication refers to the use of more than one factor to verify a user's identity. Passwords and pin numbers can still be used to confirm a user's identity, but with multifactor authentication, both the user and financial institution to authenticate each other [34].

At the very least, banks should introduce two-factor authentication systems to ensure secure log on validation [15, 22, 25, 33]. An example of a system that affords good user acceptance uses the user's registered mobile phone to receive an activation code [26]. Then, users would need to identify themselves to the bank with their account user name. Next, the bank generates a random temporary password and sends it in a short text message (SMS) to the user's registered mobile phone number [26]. Next, the user enters this challenge code into the browser and proves thus that he or she has access to the correct mobile phone [26]. This two-factor authentication works fine and is quite convenient for most users. Due to the high penetration rate of mobile phone users, there is therefore no additional hardware or cost that is incurred [26]. Apart from that, stronger authentication schemes such as the use of image marks or skins should be employed to make it more difficult for perpetrators to circumvent security controls that are currently in place [26].

Users should be trained to spot phishing when it occurs to mitigate its risk. Butler [15] outlines several simple yet effective anti-phishing measures that users can look out for when transacting online to prevent phishing attacks. Among the key aspects that users should look out for are:

- *E-mails are relatively insecure and could be easily compromised by perpetrators.* Many legitimate companies usually do not use e-mails to solicit personal details. Even if there is a need for the bank to communicate directly with the user, the recipient should be addressed by name and not 'Dear valued customer'. This indicates that the e-mail was sent in bulk thereby rendering it more susceptible to phishing. Due to this, it is best if users do not ever disclose personal and sensitive information via e-mails. When in doubt, it is best that for the user to contact the bank directly to verify the authenticity of the e-mail.
- *Poor language use and grammatical mistakes should not happen in official business communication.* Users should be on the look out for language and grammatical mistakes in the email communication they receive. This is because most banks would ensure that all public communication materials are checked and proofread to eliminate embarrassing mistakes. If there are glaring mistakes in the e-mail, there is no harm in checking its authenticity.
- *Retype the entire URL directly into the web browser to visit a site.* Alternatively, add this site's address to the favourites list and use it whenever visiting to the particular web site. Where possible, do not cut and past a link provided in e-mails.
- *Ensure that the URL of the web site is not disguised.* Many users have fallen into the trap of not paying adequate attention to the URL of the web site they are browsing. It is important to ensure that the URL is not disguised. Phishers can place the "active" part of the URL at the end of a long string, obscuring it from view. For example, most browsers ignore characters preceding the @ symbol in a URL. Clicking on www.bank.com@phishing.com, will link users to the website of Phishing,com and not

that of the bank. Users should also look out for the substitution of similar-looking characters in the URL; the intentional addition, omission or transposition of letters or the addition of certain hyphens or dots marking.

- *Make sure the web site is secure and legitimate.* Pay attention to the address being displayed on the address bar to ensure that it is 'https' and not only 'http'. A padlock icon should appear on the status bar to indicate that the web site is secure. Double-click on these locked icons to display the security certificate of the web site and ensure that the credentials listed are accurate and correct.
- *Maintain a sound password policy.* Constantly purge and change passwords to ensure its integrity and ensure that they are of a sufficient length, is alphanumeric and is not something that can be easily guessed or linked to the password owner. In addition, when prompted for a password while it is best that users provide an incorrect password in the first instance as a phishing site will accept the incorrect password, whilst a *bona fide* web site will inform the user that an incorrect password has been provided and not accept it.
- *Do not trust all emails coming from unknown sources.* If an e-mail is received from an unknown source, it is best to exercise caution and delete them immediately if they appear suspicious. Where possible, use attachment blocking and never view, open or execute any e-mail attachment unless the purpose and source of the attachment is known.
- *Regularly check financial account activity and statements for unauthorised charges*. If statements are not received timely, contact the bank to confirm the billing address and account balances, as identity thieves often change billing addresses to delay detection of fraudulent transactions.
- *Protect the computer from viruses and e-mail spam*. To protect the computer from viruses, firewalls and anti-virus software should be installed. After installing anti-virus software, it is very important to ensure that they are regularly updated with the latest virus patterns and patches. E-mail spam filters are useful in reducing the number of fraudulent and malicious e-mails that usually flood the mailbox.
- *Install anti-phishing toolbars to safeguard against phishing attacks*. These special purpose toolbars are used to determine whether a web site is safe and provide warning to users if the authenticity and security of the web site the user is browsing is suspect.

By practicing these guidelines, users are able to minimize their exposure and risk to phishing. However educating users on these issues is a challenge and requires a concerted effort by all stakeholders. Emigh (2005) adds that user education and awareness programmes should be developed based on the concerns of consumers themselves. It should be noted that better user education is one of several components that are each vital to a comprehensive action plan against phishing [22, 28]. As phishing evolves from exploiting social engineering tactics to using technology to take over the use of computers without their knowledge, solutions must also focus on the business side of the equation, such as by implementing 'secure by design', black lists and other technical improvements [9, 22, 35].

Among some of the key factors in user education is the development of consistent, clear and simple messages that could be easily understood, thereby leading to learnable actions [22]. Examples of these messages include '□Don't enter personal information on web sites', '□Don't click on URLs in email messages' and reminding users to check through other channels, such as a phone call or a visit to the official Web site, before trusting any suspicious-seeming communication [22]. Each of these messages may appear overly simplistic but nonetheless effective in combating phishing attacks. Whilst these measures may result in a marginal loss in the efficiency and gains realized by Internet banking, many organizations are reviewing the way they conduct their businesses and have opted to put consumer safety first [22]. An example would be the move by local banks to stop sending e-mails to users asking them to click on links to take advantage of promotions or update their account information.

It is also important not to give consumers the false impression that there is a 'silver bullet' that will protect them from phishing [22, 28]. For instance, encouraging consumers to type in a known URL rather than clicking on a link in an e-mail might protect them from the classic

phishing attack but not from pharming [20, 28]. Therefore it is highly crucial for those experienced in consumer education to select one or a few clear messages to address the large and growing phishing risk [16].

Based on a research conducted by Ponnurangam et al.[36], it is found that users learned more effectively, retained and transferred more knowledge in avoiding phishing attacks when training materials are presented after they fall for phishing emails that insists them to click on a link to visit a web site, login, and provide personal information. According to the study, if users were frequently trained on phishing emails, they should be able to identify other types of phishing emails in future.

With all these education programmes highlighting the need for safer Internet banking, many parties are concerned that it may end up frightening users from conducting their banking transactions online [22]. As such, educators needs to ensure that their educational messages remain positive and constantly highlight the benefits of Internet banking and the need for users to remain vigilant to realize the benefits of this handy innovation [16, 17].

Apart from users, there is also a need to educate other stakeholders in the industry and crime prevention about phishing[16, 22]. Law enforcement and consumer protection experts need to understand the phishing issue better. Technical personnel also need to understand the broader legal and policy implications of phishing [22, 28]. Only when all players involved in the Internet banking sector fully understand the phishing lifecycle and the problems posed by phishing including ways to prevent it from occurring, the likelihood of circumventing the occurrence and reducing the magnitude of phishing attacks will be greatly realized [19, 22].

The need for enhanced consumer education about phishing and related risks such as downloads of spyware and other deceptive software is obvious but this will require substantial resources and commitment from industry players [22, 35]. Time, money, expertise and effort would need to be expended to ensure that the education and awareness programmes devised achieve its intended objectives [9, 22]. Various communication methods and media such as traditional public-service announcements (PSA) on television or over the radio, Internet-based PSAs, and new tutorials that teach users how to conduct safer Internet-based banking transactions in the related contexts [22, 23]. Educational efforts to address phishing and its variants should be part of a larger strategy to have a safer Internet experience and reinforce consumer trust in all online activities, not only confined to Internet banking alone [22, 25]. To achieve breakthroughs in creating a more-informed user population, there must be clear, consistent messages and consensus to use them, innovative ways of delivering the educational information in context and funding to enable third-parties to help communicate those messages to users [19, 22, 32, 35, 37, 38].

6. Conclusion

The promise of Internet banking in lowering transaction cost and being able to reach the masses can and will only be realized when users trust the online transaction system and the transaction risks mitigated if not removed. Phishing is the major culprit in the erosion of user trust of Internet banking transactions, with numerous deceptive e-mail phishing attacks on unsuspecting users being reported in the past few years. Unfortunately many victims end up disclosing their personal details to these perpetrators, resulting in considerable financial and emotional losses. With adequate appreciation of the workings of a phisher and the phishing lifecyle, it becomes evident that apart from technical countermeasures on phishing prevention initiatives, industry players need to educate their users on the risks of this menace to reduce the consequences on victims. This paper emphasizes that proper education and awareness of phishing among users is able to minimize the negative effects customers might suffer as a result of phishing, and therefore regain the trust of users in innovative banking channel.

7. References

[1] T. Kuisma, T. Laukkanen, and M. Hiltunen, "Mapping the reasons for resistance to Internet banking: A means-end approach," *International Journal of Information Management*, vol. 27, pp. 75-85, 2007.

[2] T. Ramayah, Muhamad Jantan, Mohd Nasser Mohd Noor, and P. L. Koay, "Receptiveness of Internet banking by Malaysian Consumers," *Asian Academy of Management Journal*, vol. 2, pp. 1-30, 2003.

[3] S. Lichtenstein and K. Williamson, "Understanding consumer adoption of Internet banking: An interpretive study in the Australian banking context," *Journal of Electronic Commerce Research*, vol. 7, pp. 50-66, 2006.

[4] S. Fox and J. Beier, "Online Banking 2006: Surfing to the Bank," Pew Internet & American Life Project, USA 2006.

[5] H.-B. Ong and M. Y. Cheng, "Success factors in e-channels: the Malaysian banking scenario," *International Journal of Bank Marketing*, vol. 21, pp. 369-377, 2003.

[6] J. N. Sheth, "Psychology of innovation resistance: The less developed concept (LDC) in diffusion research," *Research in Marketing*, vol. 4, pp. 273-282, 1981.

[7] B. Suh and I. Han, "Effect of trust on customer acceptance of Internet banking," *Electronic Commerce Research and Applications*, vol. vol 1, pp. pp. 247-263, 2002.

[8] R. Becker, M. B. Schmidt, and A. C. Johnston, "Mitigation of identity theft in the Information Age," in *Encyclopedia of Information Security & Ethics*, M. Quigley, Ed. New York: IGI Global, 2008, pp. 451-456.

[9] O. Mahmood, "Dilemmas of online identity theft," in *Encyclopedia of Information Ethics and Security*, M. Quigley, Ed. New York: IGI Global, 2008, pp. 143-149.

[10] N. Swartz, "Identity theft victims skyrocket, victims say," *Information Management Journal*, vol. 39, pp. 16, 2003.

[11] IMJ Staff, "ID thieves more likely to use dumpster, phone," *Information Management Journal*, vol. 39, pp. 20, 2005.

[12] MyCERT, "Computer Crime Statistics," vol. 2008: MyCERT, 2008.

[13] Ahmad Nasir Mohd Zin and Zahri Yunos, "How to make online banking secure," in *The Star*. Kuala Lumpur, 2005.

[14] L. Foley and J. Foley, "Victim resources: Victim guide," vol. 2007, 2005.

[15] R. Butler, "A framework of anti-phishing measures aimed at protecting the online consumer's identity," *The Electronic Library*, vol. 25, pp. 517-533, 2007.

[16] Madinah Mohd Saudi, Shaharudin Ismail, Emran Mohd Tamil, and Mohd Yamani Idna Idris, "Phishing: Challenges and Issues in Malaysia," *The International Journal of Learning*, vol. 14, pp. 79-88, 2007.

[17] S. Kierkegaard, "Swallowing the bait, hook, line and sinker: Phishing, pharming and now rat-ting!," in *Managing Information Services in Financial Services* H. R. Rao, M. Gupta, and S. J. Upadhyaya, Eds. USA: IGI Publishing, 2008, pp. 241-253.

[18] A. Litan, "Phishing Attack Victims Likely Targets for Identity Theft," in *Gartner First Take* vol. FT-22-8873: Gartner Research, 2004.

[19] M. Gupta and R. Sharman, "Pharming attack designs," in *Encyclopedia of Information Ethics and Security*, M. Quigley, Ed. New York: IGI Global, 2008, pp. 520-525.

[20] P. Kumaraguru, Y. Rhee, A. Acquisti, L. F. Cranor, J. Hong, and E. Nunge, "Protecting People from Phishing: The Design and Evaluation of an Embedded Training Email System," in *Computer/Human Interaction 2007*. San Jose, USA, 2007, pp. 905-914.

[21] B. B. Bhagat and L. Kharb, "Phishing and Its Indian Perspective," *The Internet Journal of Medical Informatics*, vol. 3, 2008.

[22] National Consumers League, "A Call for Action - Report from the National Consumers League Anti-Phishing Retreat," Washington DC 2006.

[23] A. Kumar, "Phishing – A new age weapon," OWASP 2006.

[24] N. P. Singh, "Online Frauds in Banks with Phishing," *Journal of Internet Banking and Commerce*, vol. 12, 2007.

[25] Zulfikar Ramzan and C. Wuest, "Phishing Attacks: Analyzing Trends in 2006," in *Fourth Conference on Email and AntiSpam*. Mountain View, California, USA, 2007.

[26] C. Wüest, "'Phishing In The Middle Of The Stream' - Today's Threats To Online Banking," Symantec Security Response, Dublin 2005.

[27] W. D. Folsom, M. D. Guillory, and R. D. Boulware, "Gone phishing," *Business and Economic Review*, vol. 52, pp. 29-31, 2005.

[28] A. Emigh, "Online Identity Theft:Phishing Technology, Chokepoints and Countermeasures," Identity Theft Technology Council, USA 2005.

[29] N. M. N. Dinna, Y. B. Leau, S. A. H. Habeeb, and A. S. Yanti, "Managing Legal, Consumers and Commerce Risks in Phishing," presented at World Academy of Science, Engineering and Technology Conference, 2007.

[30] P. Gerard and J. B. Cunningham, "The diffusion of Internet banking among Singapore consumers," *International Journal of Bank Marketing*, vol. 21, pp. 16-28, 2003.

[31] Y.-S. Wang, Y.-M. Wang, H.-H. Lin, and T.-I. Tang, "Determinants of user acceptance of Internet banking: an empirical study," *International Journal of Service Industry Management*, vol. 14, pp. 501-519, 2003.

[32] T. Pikkarainen, K. Pikkarainen, H. Karjaluoto, and S. Pahnila, "Consumer acceptance of online banking: an extension of the technology acceptance model," *Internet Research*, vol. 14, pp. 224-235, 2004.

[33] R. L. B. Stevenson, "Plugging the 'phishing' hole: legislation versus technology," *Duke Law and Technology Review*, 2005.

[34] R. G. Brody, E. Mulig, and V. Kimball, "Phishing, pharming and identity theft," *Academy of Accounting and Financial Studies Journal*, vol. 11, pp. 43-56, 2007.

[35] A. Mukehrjee and P. Nath, "A model of trust in online relationship banking," *International Journal of Bank Marketing*, vol. 21, pp. 5-15, 2003.

[36] K. Ponnurangam, R. Yong, A. Alessandro, C. Lorrie Faith, H. Jason, and N. Elizabeth, "Protecting people from phishing: the design and evaluation of an embedded training email system," in *Proceedings of the SIGCHI conference on Human factors in computing systems*. San Jose, California, USA: ACM, 2007.

[37] S. Rotchanakitumnuai and M. Speece, "Barriers to Internet banking adoption: a qualitative study among corporate customers in Thailand," *International Journal of Bank Marketing*, vol. 21, pp. 312-323, 2003.

[38] D. Ribbink, A. C. R. van Riel, V. Liljander, and S. Streukens, "Comfort your online customer: quality, trust and loyalty on the internet," *Managing Service Quality*, vol. 14, pp. 446-456, 2004.