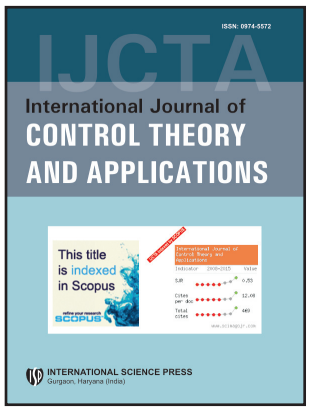

International Journal of Control Theory and Applications

ISSN : 0974-5572

Volume 10 • Number 25 • 2017

A Qualitative Exploration of Phishing and its Affect to Trust in Online Banking

Anitawati Mohd Lokman[a], Siti Sarah Md Ilyas[b], Khairul Khalil Ishak[c] and Toshio Tsuchiya[d]

[a]*RIG KAE, Faculty of Computer and Mathematical Sciences, Universiti Teknologi MARA (UiTM), Shah Alam, Selangor, Malaysia. Email: anita@tmsk.uitm.edu.my*
[b]*Faculty of Computer and Mathematical Sciences, Universiti Teknologi MARA (UiTM), Shah Alam, Selangor, Malaysia*
[d]*Shimonoseki City University, Japan*

Abstract: Phishing attack involving online banking has been increasing over the years. The attack is seen to affect victim's sentiments emotionally, mentally and physically. The critical impact is when the victim experience psychological distress, blaming and losing trust in online banking. This paper reports a qualitative research performed to investigate the state of online trust towards online banking by phishing attack victims, and their readiness to reuse online banking after experiencing phishing attack. It proposed a set of precaution measures to prevent online phishing attack involving human and technological aspect. Semi structured interviews were conducted with five phishing victims identified through snowball techniques. The results of descriptive qualitative analysis showed that the victims have lost their trust in online banking despite of being heavily reliant to the service prior to the attack. Four of the victims are reluctant to use online banking after the phishing attack. Meanwhile, one victim is still loyal to online banking due to convenience. The research result indicated that although online banking is not directly cause harm the victims, but the perpetrator used online banking as the platform to commit malicious attack. Low online trust towards online banking influenced the user's loyalty and interest in online banking. This provides insight to the crucial need for further work to develop anti phishing engine and application to detect phishing threat in online banking. The absence of such technology could lead to unsustainable facility, disrupt online trust and become a threat to the lifespan of online banking.

Keyword: Corritore's Online Trust Model, Online Banking, Online Trust, Phishing.

1. INTRODUCTION

In this digital era, monetary transactions are done online and people always update their personal information over social media. Combined, these become great opportunity for perpetrators to obtain personal details. There are millions of cybercrime cases reported worldwide every year, where the modus operand usually catch internet users off guard and ended up being victim. Malaysia is listed among one of the countries that have high-risk for online fraud [1]. In 2014, Malaysia recorded 2,993 web phishing cases involving online banking [2]. Online

banking industry in Malaysia generally has good security measures with secured network perimeters, strong security controls, regular third party audits, and two level authentications integrated to provide the best security features to protect users. However, the user themselves are not precautious and thus highly exposed to cyber fraud [3]. The common attack are phishing email and fake website. The perpetrators modus operandi begins with creating fake websites and send phishing emails to lure the victims. The fake website interface appears to be very convincing that users are incapable to discern the fake website from a legitimate website. No. matter how much banks are trying to secure their customers' online transactions, perpetrators always invent new ways to steal their personal information and ultimately their money. Online users build trust to online environment based on the assurance to be protected from undesirable occurrence [4]. Once the environment is ruptured by an external factor, the trust level of online user will diminish. Phishing attack is one example of the external factor in online banking environment in Malaysia. Phishing attack could affect the online banking users in many ways such as emotional distress, financial struggle and social interaction [5]. It influences victims differently as they could come from diverse demographic background. For instance, a housewife in India committed suicide in June 2016 after being scammed for 11 million Rupees [6]. Psychological research suggests that human naturally intuitionally judge a subject or incident based on experience rather than proved theoretical fact [7]. People are always blaming the circumstances they experienced without evidently find the cause of the incident. In phishing attack, the victims tend to transfer the responsibility to the banks, in accordance to their incapability to provide a secured online banking. However, the act is normally originated from the trauma experiencing phishing attack. Consequently, the victims of phishing attack might lose their trust to interact with online banking and they might refuse to return to online banking environment.

This paper reports a work done to investigate trust in online banking, and explore how it affects future intention of use by the phishing victims in Malaysia.

2. THEORETICAL BACKGROUND

The term "phishing" was originated from the analogy that the cyber criminals want to fish the victim like they were fishing in the sea. Hackers coined the term 'phishing' from the word 'fishing'. Phishers sent email to 'phish' the victim out of the sea of internet for their passwords and financial details [8]. Phishing is an activity of social engineering in which a perpetrator named phisher, illegally obtained internet user login credential by creating fake website imitating the real website [9],[10]. Originally, phishing involves the use of electronic mail messages such as email, designed to imitate messages from a trusted agent, such as a bank, auction site, or online commerce site [11]. Phishing attack involving online banking is common worldwide and still manage to trick the victims until recent years [1]. One of the famous case of phishing attack occurred in the United Kingdom where three men were sentenced to 20 years of imprisonment. Another famous case of phishing attack occurred in 2009 in the United States where the investigation concluded with estimation of total $1.5 million loss and the offenders received 20 years of jails sentence [12].

Other than stealing banking information, the perpetrator of phishing attack might use the obtained information through phishing scam for further victimization. The criminal may even use the sensitive information to masquerade the victims and perform fraudulent activities. Victims may even be depicted to possibility of becoming suspects in crimes committed by a criminal using their identity or credentials. Victims' personal and career life may be influences in broad range of impact such as emotional distress, financial loss, social consequences, business consequences and lost productivity [13]. Phishing incidents can cause a significant emotional distress including of denial, loss of trust, frustration, fear, anger, helplessness, embarrassment, sleeping disorder and depression. A phishing victim was found dead due to depression from losing money [14]. In some cases, the perpetrator manages to obtain all the money from the victim's saving account. This will cause the

victim lose the source to support themselves and could not afford to fulfil their financial commitments in term of social aspect, phishing incidents can cause tension on personal relationship and tarnished the victim's reputation. Time duration to recover from phishing differ from individuals and some victims might take months or years to gain their confidence to join the society again. During the time to recover from phishing, the victim might need to take a break from work resulting the loss of productivity causing the colleague and higher management to take responsibility on the workload. Lastly, phishing attack also can affect an organization's reputation. Most of phishing modus operand use an established organization's name to lure the victims. After being tricked, the victim might have a bad impression towards the organization even though the organization is not involved the scam. It can be said that the organization itself is an indirect victim of phishing. The organization unknowingly will lose their customer and get their reputation tarnished by irresponsible individuals.

Phishing threat usually target the victim by manipulating the victim's phycology. Phishers use visual deception [15] to imitate legitimate text, images and windows. Visually deceptive text tricked the users by changing the syntax of a domain name or known as type jacking attacks, which substitute letters structure in the domain name [16]. For example, the URL for Maybank2u is 'www.maybank2u.com' and the phisher will change it to 'www.maybank2uu.com'. Phishers have also taken advantage to type jack the non-printing characters and non-ASCII Unicode characters in domain names. Phishers are also bound to use an image of a legitimate hyperlink to navigate the user to a scam site [17]. Another common trick to deceive user is the underlying window masks where multiple fake browser windows place layered or next to a legitimate window [18]. Users may mistakenly trust that both windows are from the same source, regardless of deviations in address or security indicators from the legitimate site. In the worst scenario, a user may not even notice that the multiple layered window appeared on the screen. Lastly, the deceptive look and feel of the website [18],[19]. Phisher creates a fake website with the exactly same interface design, layout, logos and functionality. Consequently, the user unknowingly giving the credential details to the perpetrator.

Online banking has gain wide acceptance in Malaysia due to the change of their lifestyle [20]. The fast-paced world these days require salarymen to work more than 8 hours a day and have No. time for leisure. Unable to go out, they find the initiative to buy things online to save their time. Other than that, most online shoppers are women [1], [21]. Women loves to keep up with trend and buy the latest clothing and item. Hence, businesses came up with the ingenuity to expand the online shopping facility in Malaysia. Social media has also played important role as virtual store to assist and promote products to potential customers. The technology advancement and internet access are the factors contributing for this growth [22]. Information Technology (IT) as enabler has given the spurt to online banking evolution in Malaysia. Without the devices and internet, the user are not able to access online banking aligned with the IT literacy possessed by youth nowadays. In 2014 there are 6 million people who used mobile banking. This is mainly due to the mobility offered by apps over smartphones [22]. Hence, progressively online banking users prefer to use mobile phone or tablet to perform banking transaction.

Online banking user in Malaysia agreed with the ease of use of online banking system [23] and stated the significance of computerized self-service finance. It can be accessed anywhere anytime if the user devices are connected to the internet. Moreover, online banking promotes a hassle-free service. Users can perform transactions without waiting for turns. From the bank institution side, online banking helps the bank to promote customer confidence, reduce operating cost and manpower and achieves more efficient and enhanced financial performance [23].

3. METHODOLOGY

The research adopted Corritore's Online Trust Model to emphasize on the perception of trust influenced by the credibility, usability and risk factors. External factor in online environment is added to the model, as the

preliminary investigation indicated that external factors can affect trust of online users towards the regular online web or application that they used. Snowball sampling method is used as the study interest is of respondent from limited and unknown population. Although phishing attacks happened, it is difficult to find the victims as banks refused to disclose victims to protect privacy and moreover the bank's reputation. Thus, snowball technique was used to identify the population of phishing victims. The sampling works by firstly identifying the initial subject for the research. Then, the researcher asked assistance from the subject to help identify people with a similar trait of interest. The process is repeated until the there is No. more possible respondent.

Semi-structured interview was conducted through face to face meeting and phone calls. Each informant was interviewed in two sessions on different day. Each interview took 40 minutes to one hour to get as maximum input from the informants. The level of data saturation varied depending on the study design where No. new data, No. new themes, No. new coding can be obtained from the informant. In each session, similar but paraphrased questions were asked to the respondents to validate consistency of the data. New topic discovered during the first session of the interview were added to the second session interview questions. This is to ensure the interview reach data collection saturation to achieve the research objectives. A total of 22 questions were asked based on the adopted Corritore's Online Trust Model. The data obtained from the interview is used to look for patterns and comprehend the insights of the respondent's experience. Descriptive qualitative analysis was performed to gain understanding of underlying reasons and motivations. In the analysis, the informants were named Informant 1, Informant 2, Informant 3, Informant 4 and Informant 5. All answers from 22 question asked in the interview were analysed qualitatively to understand the input given by the informants.

4. FINDINGS AND DISCUSSION

The keywords observed from the informants' first impression towards online banking were efficiency, time saving, convenience and ubiquitous. This indicates that the informants perceived online banking positively prior to a phishing attack. The perception of trust towards online systems depends on the emotional acceptance of its user in terms of credibility, ease of use and possible risk. The informants found online banking to be easy to use and they believed the internal system of online banking is safe.

This shows that the informants have stable trust towards online banking. Online banking gain its trust as it promotes ease of use, credibility and low-risk for cybercrime. Emotionally, the informants agreed that online banking can be trusted if No. fraudulent event occurs when using online banking. Prior to the attack, the informants trusted and depended much on online banking. The informants have mixed feeling after being recognized as the victim of phishing attack while using online banking. Table 1 shows the keywords of the victim's emotional state after phishing attack. Four of the victims were angry since the incidents involves privacy concern and monetary issue. The victims also considered the bank was responsible for the unfortunate incident even though the bank has provided its user with a good security measure before login into their online system.

Table 1
Emotional Effect to the Victims

Informant	*Keywords*
1	"…shocked…angry…blame the bank…then blame myself"
2	"…accept the reality…"
3	"…angry…betrayed…
4	"…angry…blame myself…"
5	"…angry…depressed…"

Phishing attacks incidents has left a huge impact to the victims as most of them has suffer monetary lost that they saved for their future life. The scam attack by the irresponsible party has tarnished the reputation of online banking as the banking alternative to the traditional banking. The informants were asked question to identify their willingness to use online banking after being a victim to phishing attack. Table 2 tabulate the result of the question analysis. The keywords indicate negative responses from the informants leading to distrust towards online banking. Four respondent decided to stop using online banking. The reason of their judgement includes loss of trust and traumatic to the incident. However, the informants agreed human factor and technology has equal responsibility in enabling phishing attack

Table 2
Readiness of Victims to Use Online Banking

Informant	*Keywords*
1	"...deactivated online banking…lost trust…"
2	"…not going to use…traumatic…"
3	"…still use…convenient…"
4	"…stopped…prone to attack…"
5	"…no…best way to avoid phishing…sceptical…

Human mindset has cognitive practicalities of the impulse to blame [7], and human tend to transfer the responsibility to other party whom indirectly involve in the process. Literature review depicted that phishing can cause emotional distress to the victims. The results from the analysis shows that the informants also were emotionally upset after being tricked by phishing attack. The incidents caused the victims grievances and stress. In this research, phishing attack is declared as the external factor to online trust. External factor defined as the outside attack that could rooted distrust in online banking. Phishing attack is initiated by perpetrator that use online banking as the medium to convince the victims. Logically, online banking is not the one who steal the money from the victims. However, the indirect involvement of online banking in the incident has affecting the victims' perceptions in online banking. This is because the bank's image has been used to attract the victims and the trust level made the victims undoubtedly to follow the instruction from the perpetrator.

The analysis on the willingness of the victims to use online banking after phishing attack show that four out of five informants stopped using online banking. One informant still attached to online banking. The factor leading them to stop using online banking deduced as the loss of trust towards online banking. The informants were sceptical on the security issues of online banking since it was involved secondarily in the phishing attack.

5. CONCLUSION AND RECOMMENDATION

This research produced a set of precaution measure to help prevent phishing attack. The precaution measure was developed based on the data obtained from the informants. Exploratory result from this research suggest that the precaution measure should be developed for both online banking user and the bank itself. Mutual initiative would be the best solution to reduce the phishing threat. Collaboration with authorities responsible for cybercrime is encourage to support the bank resolution to fight with phishing attack.

From user side, the research result suggest that the user should be educated on phishing attack and how to handle it, be cautious of suspicious email, use Private Browsing tab and install suitable antivirus or anti phishing application. The most common phishing attack is via email; where the perpetrators will send email impersonating a legitimate organization. Phishing email usually contains instruction for the victims to reveal their personal formation. Online banking users should be cautious if any unknown source send a suspicious email. As a safety measure, users should contact the respective bank representative to clarify if the bank has release such email to

customers. Upon confirmation with the bank representative, delete the email if the bank did not acknowledge the email release. Legitimate organization usually does not communicate with its customer via email for any procedure. Spam email also contains a phishing URL.

Online banking user also should learn on how to determine legitimate URL, before accessing online banking website. There a few ways to identify phishing URL. The first one is to identify the host and domain name. Phishing URLs usually contain unknown host name, large host name or misspelled domain name. It will be hard for user with low IT literacy to identify phishing URLs. Hence, they can identify phishing URLs by checking if the URLs start with 'https://'. The easier way is to spot the SSL padlock icon the left side of the address bar. In a nutshell, the user should allocate their time to explore on information regarding phishing attacks. The user can use the benefit of internet to search for relevant articles on phishing attacks and visit CyberSecurity website to get the latest information on cybercrimes in Malaysia. CyberSecurity is glad to serve Malaysian to raise the awareness on the downside of cybercrime.

Other than that, online banking user is advised to use private browsing tab to access online banking. Private browsing is a feature embed in all web browser to enable online user to have a safe browsing experience. Private tab will not keep the user browsing history. It also disable the storage of cookies and web cache. This feature is developed to keep the privacy of user browsing history. Hence, outside party cannot secretly tracked or monitor our online trace. It is advisable for online banking user to use private browser when accessing online banking.

Installing antivirus in personal computer could help online banking user to detect suspicious link. Antivirus nowadays is equipped with the technology to detect suspicious URL and check the validity of the URL before directing the user to the selected page. Then, if suspicious URL is detected, the antivirus will notify. A lot of reliable antivirus can be obtained in the market such as Kaspersky, McAfee and Avast. Online banking user also can download the trial package available at the antivirus official website.

Online banking user also should install DontPhishMe, a web browser plugin for Mozilla Firefox and Google Chrome. DontPhishMe was developed by MyCERT, CyberSecurity Malaysia to provide online banking user with a security mechanism in averting online banking phishing threat. PhishMe alerts the user if an online banking website request personal or financial information under false deceptions. DontPhishMe will automatically warn the user if the visited website is suspicious. DontPhishMe was granted an award from Softpedia, acknowledging it is free from spyware, malware and viruses. DontPhishMe support almost all online banking website in Malaysia including Maybank2u, CimbClicks, Public Bank, Bank Rakyat, Bank Islam, HSBC, EON Bank, UOB, AMBank, OCBC, RHB, Citibank, Standard Chartered Bank, al., Rajhi Bank, Affin Bank, Hong Leong Bank, Alliance Bank, BSN, Muamalat and Kuwait Finance House [24].

From the bank side, the bank should take the initiative to launch operation to monitor the fake websites cloning the official website available online. Usually, fake website will obfuscate the URL to make it look similar to the legitimate URL. The bank can report the identified websites to MyCERT for further action. The cooperation between the bank and MyCERT is necessary in order to have elimination of fake website. This kind of initiative is beneficial to both online user and the bank itself. The user may have less possibility to be exposed to malicious threat. The bank also can safeguard their reputation among its user.

MyCERT, CyberSecurity Malaysia has commenced DontPhishMe to help online banking user to have a safe experience to access online banking website. Other than that, MyCERT also has launch CyberSafe campaign aimed to raise awareness of online scam attacks. This campaign implemented through roadshows to educate the public mostly kids to recognise online scam and how to protect themselves. However, the initiatives by MyCERT is widely known to the public. MyCERT should promote the initiatives through social media. Social media platform has now become the medium for information sharing. Information dissemination spread faster

within social media environment. MyCERT has share a lot of information regarding cyber-attack in their website. They always release advisories and articles related to cyber security. They also always updates the recent cyber fraud activities over the internet. MyCERT also use Facebook to update online user on cyber security and recent technology to prevent fraudulent activities attempt. However, only 1964 Facebook user subscribing to the page. MyCERT should make the page known to the public so that the online users will be aware on the existence of such services provided by MyCERT.

The above set of precaution measure provides reasonable mechanism to minimize phishing attack risk. It could benefit both users and online banking operators in terms of enhancing security in online banking, and extend the sustainability of the technology.

Acknowledgement

This work is supported by Research Management Centre of UiTM Shah Alam, Malaysia under the REI Grant Scheme (Project code: 600-RMI/DANA 5/3/REI (6/2013)). The paper is also supported by Malaysia Association of Kansei Engineering (MAKE), and Research Initiative Group of Kansei/Affective Engineering (RIG KAE).

REFERENCES

[1] A. M. Ahmad and H. Al-Zu'bi, *E-banking Functionality and Outcomes of Customer Satisfaction: An Empirical Investigation*, International Journal of Marketing Studies, pp. 50-65, 2011.

[2] Z. Aljazzaf, M. Perry, and M. Capretz, *Online Trust: Definition and Principles*, IEEExplore, 2010.

[3] A. Almomani, T. C. Wan, A. Manasrah, M. Altaher, M. Baklizi, nad S. Ramadass, *An Enhanced Online Phishing E-Mail Detection Framework Based on Evolving Connectionist System,* International Journal of Innovative Computing, Information and Control, pp. 1065-1086, 2013.

[4] S. Baskarada, *Qualitative Case Study Guidelines*, The Qualitative Report, pp. 1-18, 2014.

[5] R. Basnet, and A. L. Sung, *Learning to Detect Phishing URLs*, International Journal of Research in Engineering and Technology, 11-24, 2014.

[6] BBC News, "Suicide of Internet Scam Victim". Available: BBC News: http://news.bbc.co.uk/2/hi/uk_news/england/cambridgeshire/3444307.stm, 2004.

[7] Y. Y. Beh, , T. Faziharudean, *Factors Affecting Customer Loyalty of Using Internet Banking in Malaysia*, Journal of Electronic Banking Systems, pp. 1-20, 2010.

[8] R. Dhamija, J. Tygar, and M. Hearst, *Why Phishing Works*, Proceeding of CHI-2006: Conference on Human Factors in Computing Systems. Berkeley, 2006.

[9] R. Elliott, and L. Robert, *Descriptive and interpretive approaches to qualitative research*, In A Handbook of Research Methods for Clinical and Health Psychology, pp. 147-160, 2005.

[10] P. I. Fusch, and L. R. Ness, *Are We There Yet? Data Saturation in Qualitative Research*, The Qualitative Report, pp. 1408-1416, 2015.

[11] S. Garera, N. Provos, M. Chew, and A. Rubin, *A Framework for Detection and Measurement of Phishing Attacks*, WORM, 2007.

[12] Hoyer, and Phillip, *Phishing Accross Interaction Channels: method; experience and best practices*, Journal of Financial Serivce Technology, 29-34, 2008.

[13] S. L. Lim, *Industy Focus: ASEAN Banks*, Singapore: DBS Group Research, 2015.

[14] J. Ma, L. K. Saul, and J. Voelker, J. Identifying Suspicious URLs: An Application of Large-Scale Online Learning. Proceedings of the 26 th International Conference on Machine Learning. Montreal: UC San Diego, 2009.

[15] A. Irsyad, *Malaysia Is Becoming A Global Hub For Online Scams, Will You Be The Next Victim?* Available: Malaysian Digest: http://malaysiandigest.com/features/583209-malaysia-is-becoming-a-global-hub-for-online-scams-will-you-be-the-next-victim.html, 2015.

[16] T. N. Jagatic, N. Johnson, M. Jakobsson, and F. Menczer, *Social Phishing*, Communications of the ACM, pp. 94-100, 2007.

[17] A. Jain, and V. Richariya, Implementing a Web Browser with Phishing Detection Techniques. World of Computer Science and Information Technology Journal, pp. 289-291, 2011.

[18] Khan, and Shahid, *Qualitative Research Method: Grounded Theory*, International Journal of Business and Management, pp. 225-233, 2014.

[19] A. Kumar, *Mobile Banking Security in Malaysia in 2015: eLock Interview*, Retrieved from Computer World: http://www.computerworld.com.my/printarticle/, 2013.

[20] M. Blasi, *Techniques for Detecting Zero Day Phishing*, Iowa: Iowa State University, 2009.

[21] J. A. Chaudhry, S. A. Chaudhry, and R. Rittenhouse, *Phishing Attacks and Defenses,* International Journal of Security and Its Applications, pp. 247-256, 2016.

[22] C. Corritore, B. Kracher, and S. Wiedenbeck, *On-line trust: concepts, evolving themes, a model*, International journal of human-computer studies, pp. 737-758, 2003.

[23] CyberSecurity, *eSecurity*, Selangor: CyberSecurity Malaysia, 2010.

[24] K. Rouibah, R. Thurasamy, and S. M. Oh, *User Acceptance of Internet Banking in Malaysia: Test of Three Competing Models*, International Journal of E-Adoption, 1-19, 2009.