International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 7, Issue 1, January 2017)

# E-Banking Security: Internet Hacking, Phishing Attacks, Analysis and Prevention of Fraudulent Activities

Alhuseen O. Alsayed[1], Anwar L. Bilgrami[2]
*Deanship of Scientific Research, King Abdulaziz University, Jeddah, Saudi Arabia*

***Abstract*--Since the introduction of internet banking to the banking sector, many users have discovered hard ways that their use of e-banking can place their financial data at risk. Therefore, security has become a frequent concern for both banks and users. A phishing attack refers to any modus oprendi to trick customers into thinking that their financial institution is requesting information from them, when in reality, the request is coming from the hacker. Phishing leads to online identity theft, because it involves an unauthorized individual or group stealing confidential data. Unfortunately, phishing attacks are among the most common criminal activities that have been conducted by hackers, since the introduction of internet banking. The objective of this research is to investigate how phishing hackers attempt to steal users' data and conduct financial fraud. In turn, it explains how bank users can secure their online transactions with security solutions.**

***Keywords*-- E-banking, security, phishing attack, countermeasures, authentication, phishers.**

## I. INTRODUCTION

The Internet has been around for decades. Many people have been using the internet to facilitate their lives and expedite their daily tasks [1]. Of all the aspects of daily life that have benefitted from the internet, the banking sector has been especially effective at capitalizing on internet's features. It has introduced through the internet many attractive ways to increase the scope of its financial services. The emergence of internet banking has allowed banks to offer their customers relatively convenient and flexible banking, also known as e-banking. This term does not yet have a precise definition, as many researchers have defined e-banking differently. In general, e-banking refers to bank customers using the internet to perform financial services such as financial transactions [2]. These services now come in a wide range, including but not limited to conducting fund transfers, managing a checking account, and bill payments. Additionally, e-banking enables customers to access their bank accounts through banks' websites without the need of travelling to the bank [3]. Internet banking has benefited both banks and customers. The banks are benefited because the internet has allowed banks to diminish their operational costs in terms of decreasing physical facilities involving human resources, paperwork, and supporting staff.

The customers are benefited because e-banking has given them fast access to various financial activities, such as money transfer, payment for utility bills, checking account management [4, 5].

As cited [3], bank customers can use banking in three overarching ways. The first use is to obtain simple information about services provided by the bank through its website, such as products and policies [1]. The second and third uses are simple and advanced transactions, respectively. Transactional websites are types of internet banking that enable customers to conduct simple transactions, such as account inquiry. The Simple transactions do not allow users to transfer funds. An advanced transactional website allows customers to transfer funds and access other online financial services and conduct other types of transactions. Many countries have integrated the use of the internet into their traditional banking system. Since the introduction of the internet, some of ihe banks around the world are offering internet services, for instance, Bank of America, Centura Bank, Citibank, NationsBank, etc., [6]. These banks offer their customers convenience and flexibility of use, thus contributing to the growth of the bank and popularity of e-banking.

Despite benefits that banks are offering to their customers through online services, e-banking has also raised many security issues [1]. Computer hackers have developed a variety of elusive methods for stealing internet bankers' money. Although there are many advantages of online banking, security issues often discourage customers from using it, as many customers have found that the use of online banking could leave their financial assets at risk [7, 8]. Since most banks are now offering services to their customers through the internet, an increasing number of hackers have found it worthwhile and appealing to dedicate their time to conduct frauds through online banking system. It has been observed in many research studies that security issues, such as "phishing attacks," have been used by hackers to breach e-banking customers' accounts [9, 10].

Banks will put their customers at risk and eventually drive them away if they do not strengthen the security of their e-banking. The primary services that customers use via the internet are transferring money across accounts, paying bills, checking account balances, and sending and receiving confidential information between banks and fellow customers [4].

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 7, Issue 1, January 2017)

Therefore, financial institutions should pay particular attention to protecting the information of their own organization, their users, and their finances, which are all forms of sensitive information of which hackers can take advantage. In terms of phishing, banks must protect their users' confidential data from unauthorized individuals or groups who could inquire after users' bank accounts to conduct fraudulent activities such as stealing customers' private information, data and ultimately the money. Unfortunately, the current lack of security protection amongst most online banking is conducive to phishing attacks.

This paper is divided in four major sections: section 1 has altready introduced te subject and discussed various aspects of e-banking and phishing, section 2 describes phishing attack in e-banking and explains how it works,section 3 offers security solutions, such as authentication methods, that financial institutions should take into consideration and in the section 4 conclusion are drawn.

## II. Phishing Attacks On E-Banking

The phishing attack has become one of the most common financial crimes in recent years. Phising is defined as "a criminal activity using social engineering techniques that enables phishers to attempt fraudulently acquire sensitive information, such as passwords, credit card details, national oidenticard information etc., by masquerading as a trustworthy person or business in an electronic communication [11]. Phishers can even breach the security of a bank after they access user's financial information; then, they conduct a wide range of illegal activities. Online banking users are more vulnerable to e-banking frauds, when they conduct any financial activity through the web, such as money transfer. Phishing attackers can breach the security of bank websites by using sophisticated technologies such as the Man-in-the-Middle Attack. The attackers' goal is to get access to bank users' data [12]. They then use this financial data to harvest money or conduct financial frauds for their benefits, such as funds transfer and purchasing goods. Thus, e-banking users are at risk of losing their money. Phishing attacks may include deceptive, malware, and DNS-based attacks. In deceptive attacks, hackers send a deceptive message to the bank users. The deceptive message may have some sense of urgency, such as reporting a fake account problem and a fake issue with account activation. The purpose of the deceptive message is to lure the user to interact immediately [13]. These deceptive phishing attacks will be discussed in detail in the later sections.

### *A. Man-in-the-Middle Attack*

The Man-in-the-Middle attack is a phishing technique used by e-banking phishers to conduct fraudulent activities. During Man-in-the-Middle attacks, hackers place themselves between banks and customers while customers are using their online banking accounts [14]. Therefore, both banks and end-users do not realize that the transactions are connected with the phishing attackers until money disappears without customer's authorization. Phishing attackers make use of both online banking services and lack of users' awareness about phishing techniques to breach users' security. Numerous cases have been recorded where bank users meet victims of phishing attacks when they were using online banking [10]. In addition, some users of financial institutions, such as "Citibank and other American and Australian banks", have fallen into the phishing attacks and lost money [15]. The Man-in-the-Middle attack can be combined with other types of phishing attacks, such as deceptive and malware-based phishing to commit financial frauds.

### *B. Deceptive Phishing Attack*

Deceptive phishing is another type of phishing attack that attempts to gain access to financial accounts of users. The most common method of a deceptive phishing attack is sending false notifications through email [16]. In this type of phishing attack, an attacker sends email messages to users, masquerading as one of the bank's representatives. In addition, this deceptive email contains a "call action," which means that the phisher is using a sense of urgency in order to attract recipients into clicking on a fraudulent website link included in the email [13]. If the user clicks on the provided link, the user will be directed to a fraudulent website which looks like a legitimate bank's website. Thus, the user may feel comfortable entering his or her confidential information, such as username and password. Once the user enters that information, phishing attacker collects the confidential information and can then sign into the user's banking account to conduct fraudulent activities [17]. An example is provided and illustrated in Fig. 1, how bank users could be deceived by a fraudulent website.

As shown in Fig. 1 and 2, emails that appear to be forwarded from PayPal and Citibank [15]. In these cases, the phishing attacker is using a sense of urgency to get the attention of the costumer by sounding like a report of a serious problem from a trusted source such as PayPal or Citibank. The user then clicks on the link provided in order to enter the requested financial information. The phisher collects the victim's information, because the phisher has full access to the bogus website to which they linked to the user.

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 7, Issue 1, January 2017)

Phishing attackers may then exploit user's financial information to conduct financial fraud.

Therefore, online bank users are at risk of losing their money when responding quickly to unusual emails that appear to be from their financial institutions.

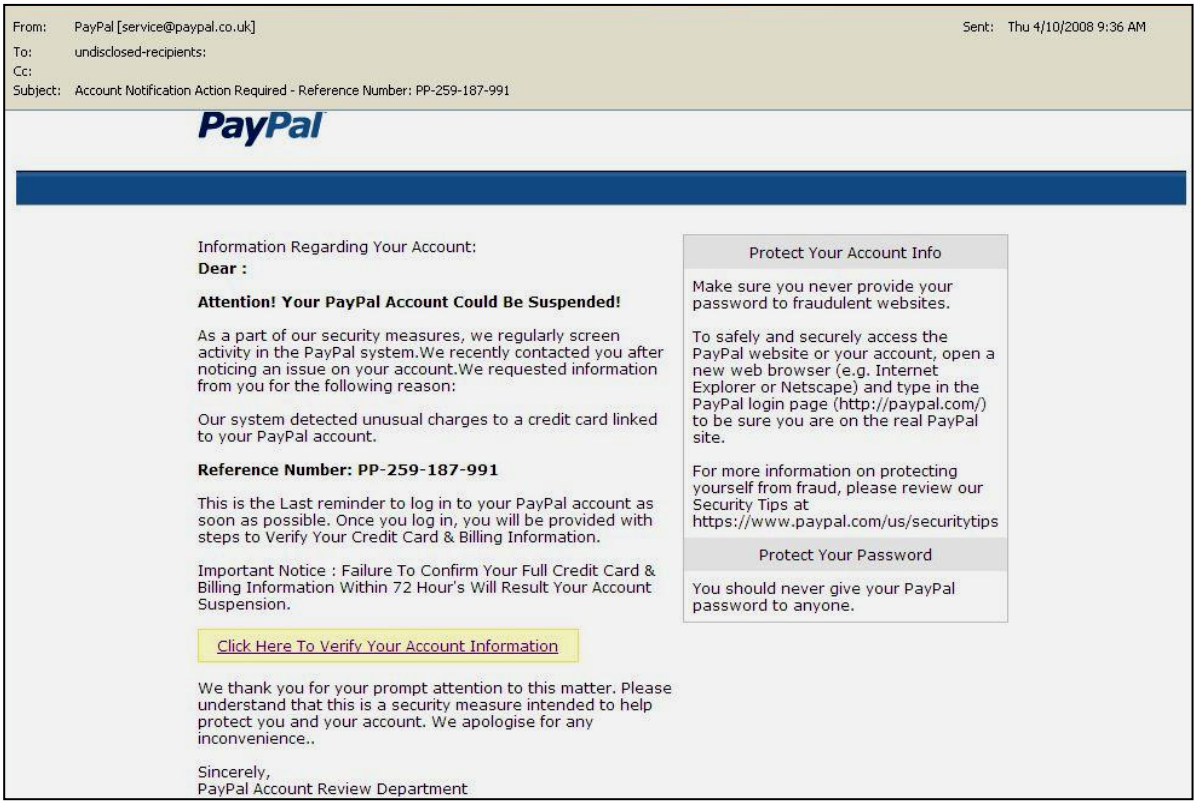


**Figure 1: Phishing Email Claiming to be from PayPal [15].**

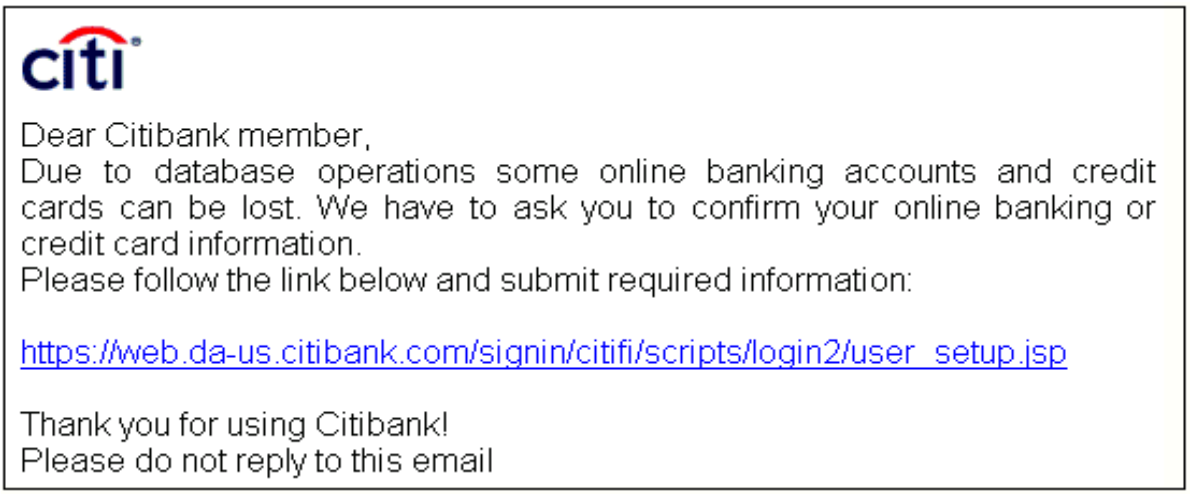


**Figure 2: Phishing e-mail claiming to be from Citibank**

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 7, Issue 1, January 2017)

As shown in Fig. 1 and 2, emails that appear to be forwarded from PayPal and Citibank [15]. In these cases, the phishing attacker is using a sense of urgency to get the attention of the costumer by sounding like a report of a serious problem from a trusted source such as PayPal or Citibank. The user then clicks on the link provided in order to enter the requested financial information. The phisher collects the victim's information, because the phisher has full access to the bogus website to which they linked to the user. Phishing attackers may then exploit user's financial information to conduct financial fraud. Therefore, online bank users are at risk of losing their money when responding quickly to unusual emails that appear to be from their financial institutions.

### *C. Malware-based Phishing*

Malware-based phishing refers to software programs that hackers install on customers' computers. This kind of phishing attack can happen when customers or bank employees visit an unauthorized website or download some infected software programs into their computers. The Phishing attackers use many techniques, such as keyloggers to gain credential information of bank users [18]. Keyloggers are programs that install themselves onto bank users' computers when customers visit any websites with a keylogger or download a piece of software with a keylogger [19]. Hackers install these types of malware-based phishing software on users' computers without their knowledge or permission. Therefore, phishing attackers find this type of malicious software easy to use for fraudulent activities, asince the victims are often unaware that such softwares even exist on their computers. When the bank user with infected computers visits their bank's website and enter their financial information, such as usernames, passwords, and token numbers.The malware logs the keystrokes that the users entered while typing in their confidential information [6]. Thus, the keylogger collects the required information and sends it to the attacker as a file. Phishing attackers borrow the keystroke information from the file to log in as the user and conduct financial fraud. Grebennikov[20] points out that many online banking customers have been victims of malware-based phishing, especially keylogging.

Grebennikov [20] further describes a typical keylogging incident, which occurred in Brazil. The hackers in Brazil used keylogger attacks as a method to collect bank users' data. These phishing attackers installed keyloggers into users' computers. The keylogger programs became active when the users visited their banks' websites, and then everything that users typed was secretly captured and sent subsequently to the hackers. As a result, a huge amount of money was stolen from private accounts in Brazil.

Another infamous fraudulent crime streak was conducted in 2005 when some hackers breached online bank security of the Bank of London and managed to steal its customers' money. Phishing attackers in this case used keylogger trojans to track customers' keystrokes [6]. These cases are just two of many other documented cases of phishing attack techniques used by hackers to steal from bank's customers. In response, financial institutions must protect users' data by finding ways to detect and block keylogging during transactions.

### *D. DNS-Based Phishing*

DNS-based phishing, or more succinctly known as pharming, is another type of phishing attack in which an online deceptive agent gains control of the bank users' data. During the pharming technique, attackers are tampering with the bank's host files or domain name system (DNS) [21]. This form of attack redirects users to a fake website when they attempt to type in the domain name of their bank's web address [13]. The hackers can perform the phraming attack in two ways. They can install a virus on the user's computer or tamper with the bank's web domain. Regardless of the method, the result is that the users type the correct URLs of their financial institutions on their browsers, but then they are directed to fraudulent but legitimate-looking websites. Therefore, users remain unaware that the websites into which they are typing their credentials are under the hackers' control.

## III. PHISHING ATTACK COUNTERMEASURES

There are various methods that a bank can use to combat phishing attacks. These methods are known as phishing attack countermeasures, which include e-mail and web page personalization, protection software, the use of two-factor authentication, and increasing customer awareness. Some of the methods that this section recommends to reduce the risk of phishing attacks will prevent the users from being fooled by online phishing attackers. Phishing attacks can be combated if both banks and users adhere to these countermeasures.

### *A. E-mail and Web Page Personalization*

This section mainly focuses on how identifiable personal information could combat the risk of phishing attacks on bank users.

### *B. E-mail Personalization*

The simplest way for banks to combat the deceptiveness of phishing attack messages is to include personalized information with all legitimate communications. Financial institutions need to implement personal identifiable information to differentiate their messages more clearly from phishing attacks [13].

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 7, Issue 1, January 2017)

All messages sent to customers should be personalized for specific recipients. Personal identifiable information may include the user's name or other references of unique information shared only between the banks and customers [22]. For example, if every email sent from the bank begins with the customer's name and this email educates the users about this practice, then the customer will know that any email which does not include his or her name should be deemed as a suspicious email. Personal identifiable information helps bank users to ensure that the email was sent by their banks. Since phishing attacks do not include the user's personal information such as a name, the deceptiveness of phishing attack can be reduced when banks implement the e-mail personalization technique. In fact, banks are now required to include personal identifiable information to safeguard their customer's credential data. The implementation of this type of technique is difficult, but it is effective.

*C. Web Page Personalization*

Another form of personal identifiable information is web page personalization. In this type of personalized information, the bank users request a text or image to be used along with their passwords and usernames. In addition, the users have to pass through two web pages when visiting their bank's website [22]. The first page requires the user to provide a username. When the user name is valid, the user is given a personalized page for entering the password. The second page is personalized with the phrases or images that the user chose when he or she created the account. The bank should remind the user never to type in his or her password unless he or she recognizes the image and/or phrases on the password page. For example, a customer of the Large Bank and Trust Company may have typed in the personalized text, "You were born in Prague," and selected or uploaded a picture of a Canadian penny. Unless this customer sees both forms of personalization on the password page, he should not give the site his password.

Emigh [13] states that The Large Bank and Trust Company has provided its customers with web page personalization wherein the users can type a unique personalized message and upload a picture to safeguard them from phishing attacks. Only the single user and the bank share this personal identifiable information. Therefore, a phishing attacker will not know this personalized information and will not be able to replicate it when attempting to forge deceptive emails or web pages [13, 22].

*D. Protection Software*

Phishing attacks are difficult to predict because they come in a variety of methods to access user computers and obtain credential information, such as usernames and passwords.

As mentioned earlier, attackers could use malware programs to infect a user's computer. This type of malicious attack could be installed when the user visits a suspicious website or downloads an email attachment. Therefore, one of the simplest tools that a user can apply to prevent phishing attacks from reaching his or her computer in the first place is the anti-virus and anti-spyware software [10]. Anti software includes computer programs that protect users from viruses and spyware by scanning the entire files. These computer programs prevent phishing attacks by detecting software that could redirect users to fraudulent banking web sites.

Another type of software that could be effective in preventing phishing attacks is anti-logger software. Since most Anti software is not sufficient in detecting keyloggers, the anti-logger software can assist with detecting hidden keylogger programs. Both banks and customers should install protection software onto their computers. Once they install these software programs, the user must enable them and ensure they are up-to-date [23].

*E. Two-factor Authentication*

Banks should use effective methods to authenticate customer identity. An older method, known as single-factor authentication, is open to compromise from phishing attacks, so hackers can bypass this authentication relatively easily. Therefore, banks should reconsider relying on single-factor authentication as their only control method, as it is not effective for high-risk transactions, which involve accessing customer information or transferring funds to other parties. A popular and stronger alternative to single-factor authentication is Strong Authentication, which is also referred to as two-factor authentication. Two-factor authentication is a method that requires the users to present two different types of evidence to establish their identity. Two-factor authentication is commonly referred to as "something a user has and something a user knows" [22].

First, "something a user has" normally involves hardware or software that provides the bank users with an electronically generated passcode or digital certificate. Each bank user has a unique passcode or digital certificate [24]. The second factor, "something a user knows," usually means a private password. Bank customers should use both factors to give themselves a strong authentication system for enabling access to critical resources, such as online banks. Two-factor authentication systems are secure because attackers face great difficulty acquiring both of these factors. The implementation of two-factor authentication is stronger and more secure than single-factor authentication, such as a password alone [22].

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 7, Issue 1, January 2017)

Phishing attacks can easily capture a user's password, so the second factor for authentication is effective at reducing phishing attacks and thus dramatically reduces the chance of online frauds.

*F. Customer Awareness*

Because most phishing attacks begin with fraudulent emails, banks should prioritize customer awareness. Moreover, customers need to educate themselves about the danger of phishing attacks. A large number of phishing attacks can be prevented if the users are alert and vigilant of the threats. Banks should assist customers with their awareness by updating them of security practices. Regular updates will ensure that customers can identify genuine emails and web sites. It is imperative that banks inform their customers of the dangers of phishing attacks and what countermeasures are available [13]. Specifically, banks must ensure that they distribute information to their customers regarding how to communicate securely with their financial institution [22].

Banks should provide guidelines for their customers, as well. The purpose of the guidelines is to inform the customer about the only ways in which the bank will communicate with them. This kind of awareness should be conducted constantly and in a way that is easy for the users to understand. Guidelines can be provided in two different ways. Firstly, guidelines can be given to the customers as documents at the time of customer registration. Secondly, guidelines can also be displayed as "security instructions" on the bank's website and shown to the customer prior to login. An example of a general list of instructions that most banks publish are as follows.

- The bank will never ask users to provide their "username, password, credit card number, full name, bank account number, etc. by mail" [13].
- Bank users should never respond directly to any emails that contain urgent requests for personal information.
- An official email messages will never contain any links or application forms to be filled in.
- Bank users should always visit the bank's website by typing the bank's address into the web browser. Moreover, users should verify that the secure website indications are present in their browsers, such as the https connection and lock icon, before entering their sensitive information into the web browser.

In addition, information that banks should give to their customers regarding phishing attacks may include the following:

- Users must have protection software to have secure bank transactions.
- Users should never send their sensitive personal data via emails.

Increasing customer awareness is considered one of the chief effective ways for banks to mitigate the risk of phishing attacks when their customers are using Internet banking.

## IV. Discussion

Online banking involves many kinds of risks. Phishing attacks can be especially damaging to both banks and users who do not take precautions against this type of security risk. Since phishing hackers use several sophisticated methods, ranging from deceptive attacks to DNS attacks, banks must update their security measures regularly [8]. Moreover, banks should ensure that the transactions between themselves and their customers are secure. Banks must use some kind of updated counter measure, such as two-factor authentication, along with other protection software programs. They will also benefit immensely from educating their customers about phishing attack risks and about the ways in which unauthorized access to the users' financial information could occur while providing the steps that they can take to protect their financial information. Bank userses need to beware of phishing attacks by learning to identify suspected phishing emails. There are some signs to identify an attack sent by email. In phishing attack, attacker may duplicate an amage of a real company, copy the name of a company or use the actual name of an employee which used to assure you that you are receiving email from the company or bank. In addision, users should not respond directily to any gift or a request of loosing an exesting bank account which may leave your data at risk. Also, bank users must check the source of information from incoming mails so that they could make sure whether it is a phishing attack. Moreover, users should know that banks never send their users an email request asking for usernames and passwords. if the users receive an email requsting for credential information, they should immediately check their bank website by typing their bank website address into the web browser. As mentioned earliar, users awareness should be the top priority of banks in term of combating the phishing attack. Phishing is rapidly growing and damaging both banks and users if they do not take precautions against security risks. Ultimately, once bank customers learn about their rights and responsibilities, they can take control of their financial well-being by changing the traditional saying, "A penny saved is a penny earned" to "A penny protected is a penny earned."

## REFERENCES

[1] Razak LT(2016). The Effect of Security and Privacy Perceptions on Customers' Trust to Accept Internet Banking Services: An Extension of TAM" Mohammed A. Al-Sharaf,"Ruzaini A. Arsha," Emad Abu-Shanab and "Nabil Elayah" Faculty of Computer Systems and Software Engineering, UMP. Journal of Engineering and Applied Sciences, 100, 545-552.

[2] Jolly V(2016). The Influence of Internet Banking on the Efficiency and Cost Savings for Banks' Customers. International Journal of Social Sciences and Management, 3, 163-170.

[3] Safeena R(2010). Customer perspectives on E-business value: case study on Internet banking. Journal of Internet Banking and Commerce. 15, 1-17.

[4] Sharma S(2016). A detail comparative study on e-banking VS traditional banking. International Journal of Advanced Research, 2, 302-307.

[5] Konoth RK, van der Veen V, Bos H(2016). How Anywhere Computing Just Killed Your Phone-Based Two-Factor Authentication. In Proceedings of the 20th International Conference on Financial Cryptography and Data Security.

[6] Vaciago G, Ramalho DS(2016). Online searches and online surveillance: the use of trojans and other types of malware as means of obtaining evidence in criminal proceedings. Digital Evidence & Elec. Signature L. Rev., 13, 88.

[7] Balk R, Yap BK, Loh C, Wong HD(2009). To trust or not to trust: the consumer's dilemma with e-banking. Journal of Internet Business, 6,1-27.

[8] Leukfeldt ER, Kleemans ER, Stol WP(2016). Cybercriminal Networks, Social Ties and Online Forums: Social Ties Versus Digital Ties within Phishing and Malware Networks. British Journal of Criminology, 9.

[9] Chiu CL, Chiu JL, Mansumitrchai S(2016). Privacy, security, infrastructure and cost issues in internet banking in the Philippines: initial trust formation. International Journal of Financial Services Management, 8, 240-271.

[10] Arachchilage NAG, Love S, Beznosov K(2016). Phishing threat avoidance behaviour: An empirical investigation. Computers in Human Behavior, 60, 185-197.

[11] Ekawade S, Mule S, Patkar U(2016). Phishing Attacks and Its Preventions. Imperial Journal of Interdisciplinary Research, 2.

[12] Junger M, Montoya L, Overink FJ(2017). Priming and warnings are not effective to prevent social engineering attacks. Computers in human behavior, 66, 75-87.

[13] Emigh A(2005). Online identity theft: phishing technology, chokepoints and counter measures. ITTC Report on Online Identity Theft Technology and Counter measures, 1-58.

[14] Swanink R, Poll E, Schwabe P(2016). Persistent effects of man-in-the-middle attacks, 23-32.

[15] Eze CU, Yih CG, Ling NT, Gan GGG(2008). Phishing: a growing challenge for Internet banking providers in Malaysia. Communications of the IBIMA, 5, 133-142.

[16] Damodaram R(2016). Study on phishing attacks and antiphishing tols. International Research Journal of Engineering and Technology, 3.

[17] Mishra R(2016). Review: Phishing Attack Types & Preventive Measures. Imperial Journal of Interdisciplinary Research, 2.

[18] Chaudhry JA, Chaudhry SA, Rittenhouse RG(2016). Phishing Attacks and Defenses. International Journal of Security and Its Applications, 10, 247-256.

[19] Arora M, Sharma KK, Chauhan S(2016). Cyber Crime Combating Using KeyLog Detector tool.

[20] Grebennikov J(2007). Keyloggers: how they work and how to detect them (part 1).http://www.securelist.com/en/analysis/204791931/Keyloggers_How_they_ work_and_how_to_detect_them_Part_1

[21] Arya B, Chandrasekaran K(2016). A client-side anti-pharming (CSAP) approach. In Circuit, Power and Computing Technologies (ICCPCT), 2016 International Conference on (pp. 1-6). IEEE.

[22] Kruegel C, Kirda E(2005). Protecting users against phishing attacks. The Computer Journal, 1-8.

[23] Zhang Y, Egelman S, Cranor LF, Hong J(2007). Phinding phish - Evaluating anti-phishing tools. Proceedings of the 14th annual network & distributed system security symposium. http://lorrie.cranor.org/pubs/toolbars.html Accessed on 04.10.2016.

[24] Sampangi RV, Hawkey K(2016). Who Are You? It Depends (On What You Ask Me!): Context-Dependent Dynamic User Authentication. In Twelfth Symposium on Usable Privacy and Security (SOUPS 2016). USENIX Association.

[25] Park J, Jung B, Choi O(2016). Two-Factor Authentication Methodology using Hybrid Face Recognition,international Journal of Control and Automation, 9, 1.