International Journal of Engineering Research and Advanced Technology (IJERAT)

DOI: http://doi.org/10.31695/IJERAT.2018.3311

E-ISSN : 2454-6135

Volume.4, Issue 8
August -2018

Cyber Security Preparation for New Emerging Markets

Haider Hameed[1] and Dr. Ghadah Al-Khafaji[2]

[1]Department of Computers,

College of Science,

al-Mustansiriyah University,

Baghdad, Iraq.

haideritsec@uomustansiriyah.edu.iq and haideritsec@gmail.com

[2] Department of Computers

College of Science

University of Baghdad

Baghdad, Iraq.

Hgkta2012@yahoo.com and Hgkta2012@ scbaghdad.edu.iq

ABSTRACT

Emerging E-commerce communities considered a good chance of threating for cybercriminals because both parties of e-commerce (Business and Consumers) are not well prepared to defend against attackers' techniques.

This research tried to measure the security knowledge level for consumers as millions of employees will be transferred from cash in hand wages into electronic payrolls which will be the first step before start using the electronic banking facilities

A questionnaire about most security threats terms introduced into 50 individuals while considered only 30, participants classified as professionals and a moderate level of commuter and internet users to examine if they prepared well to defend against possible security attacks related to managing their online banking.

The results showed that although some of the users are computer professionals (as they evaluate themselves), but the questionnaire stated that even those participants are not having enough knowledge about specific security threats which might face in next future.

Also, results showed that very poor level of possible security attack terms and techniques while special organization have demonstrated the number of attacks has been done using these techniques in 2017

The most security terms that chosen to be measure are elected carefully from different previous research in e-commerce threat fields and from real evaluator for such threats as HSBC bank.

Keywords: Online Payment, Threats to Ecommerce, Threats to Online Banking.

1. INTRODUCTION

Online payment is the major part of online business that distinguish between the online selling process and online advertisement; merchants are doing a lot to deliver the item they sell to the consumers, but when the consumer order and pay online for that product then the transaction will be made, otherwise the process is close to adopt online marketing if the payment will made late or even when it deliver to the consumer.

The big question arise here is are there an online payment facility available in the country or not? Then if it is available, there are many questions must be answered such as:

1- Are people understand the electronic payment process and happy to use it or not?
2- Are people understand the security threats against online payment system?
3- Are people have the ability to access their bank accounts electronically?

The next paragraphs will explain the electronic payment system and explain how it work, then the research will explain the threat against such system and how to encourage end users to avoid be a victim of one of the attacks related to the online payment

1.1 Online Payment system

Online payment system must need an internet to enable consumer to pay for purchased goods. Online payment systems and its security restricted are different between countries because the online payment system must follow the regulations in that country. To a degree, the online payment system does need an internet availability, electronic bank accounts and at least consumer has the ability of online access/ manage to his/her bank accounts.

Online Payment System Mechanism

(Khrais, 2015)has illustrated the most common model for online banking system, Online banking can be defined as is a "series of processes that the client logs into the bank's website through the web-browser installed on the PC and carries out various online transactions by using a private username and password".

The practical steps might be reduced to:

1. The user runs computer.

2. After the running the application designed by the bank or web-browser opened, users can access the bank's website and then enters the personal identifying number (PIN) and the password by using the keyboard.

3. The credentials (username & password) are transmitted to the bank's server.

4. The bank's server decrypts the transmitted information and processes of the user's authentication.

1.2 Potential Threats.

Online attacks usually targets end users and/or business for many reasons such as stealing money; defamation business reputation; extortion.

Threats to online payment are increasing every day, especially for new emerging markets. The main reason for ease of attacking ecommerce parities can be pointed by poor security knowledge for both ecommerce parities consumers and business owners. Increasing the attack level may damage the reputation of online money transfer leading to make people reluctance to using E-commerce.

Despite of the fact that there is a long list of attacks associated with internet, this research will consider the main attacks that related to online trade and or businesses.

1.3 The nature of attack techniques

Three references adopted in this research to clarify the security attacks to online payment system, one of them issued by bank (HSBC Bank) who run online banking transaction related to its clients, the banks opinion and recommendation about security attacks to online banking system is considered as it in the area of running the business and facing the attacks roughly every day.

The other two references represent an academic research in the field of ecommerce security and threat to online transactions.

(Miko, 2010) Classified the main vectors for online attacks into:

server-side (=bank server) ; Credential stealing ; Phishing (social engineering) ; Pharming ; Man-in-the-middle ; *Man-in-the-browser ;* Generally – attacks utilizing Trojan horses and Cross-channel Attacks.

(Khrais, 2015) Stated that major Vulnerabilities to online banking system. The research classified the online attacks into two types, internal and external attacks. Regardless of the extensive explanation of these two types, one can conclude from (Khrais, 2015)that main attacks to the online transaction belong to Internal type:

Fraud or theft; Back doors or trap doors; Employee sabotage & Errors and omissions.

From very famous international bank point of view HSBC (HSBC, 2018), most dangerous attacks can be briefed into:

Fraudulent supplier requests; Courier scams; Spoofing; Keystroke; capturing/logging and Pharming.

DOI : 10.31695/IJERAT.2018.3311

1.4 Statistics for security threats against Online Payment System

According to (Wueest, 2017), scam emails was the most dominant technique method used for distribute financial Trojans during 2016 adopting well recognized office document attachment. Botnets such the Necurs (Backdoor.Necurs), approved to sent out at least 1.8 million JavaScript these statistics represented in figure 1 below

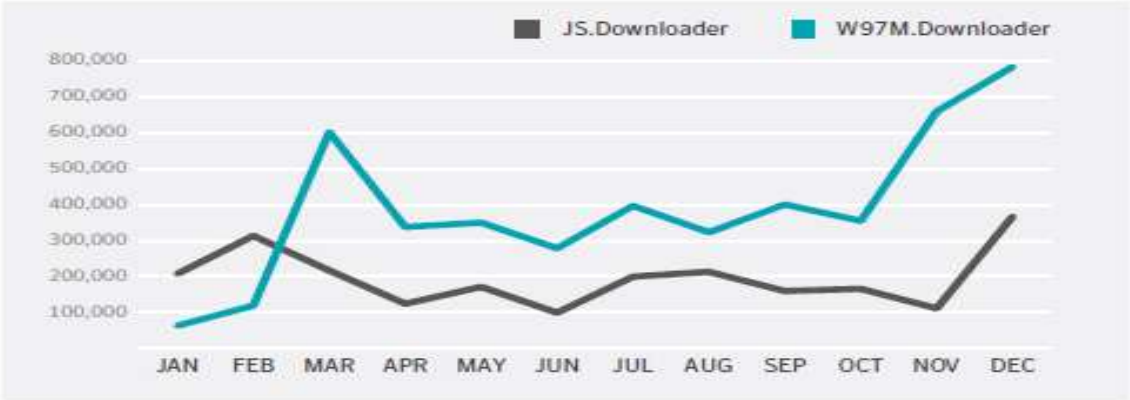

Figure 1 Document macro and JS downloader detections per month in 2016 cited on (Wueest, 2017)

1.5 Prevalence

The report of (Wueest, 2017) showed that the total number of attempted using financial Trojans minimized by more than 35% l1ast year compared to 2015 globally. The explanation for this result approved that companies succeed to stop large number of threats of spam runs.

Figure 2, Banking Trojan detection on computers 2015 and 2016 cited on (Wueest, 2017)

1.6 Social Engineering attacks

Social engineering plays a major role in financially motivated attacks, especially when need to overcoming authentication phase. The social engineering techniques used in business email compromise (BEC) scams continue to evolve. For example, attackers (scammers) register to very similar domain name and appearance to a popular website, then try to persuade legitimate users to feed their credentials (username & passwords) to the fake registration website and capture the credentials. This tactics usually used by scammers just before the day that the bank or the financial organizations send its notification email to their clients. For more information see (al-Mahmood & al-Khafaji, 2017).

2. RESEARCH PROBLEM

As emerging society, many security problems will appear for two reasons, the first one related to the lack of understanding the definitions of most attack that potentially can face the end users, the second reson will be how to deal with the attacks if happen "what is the Incident response plan available for end user". In order to test these two factors, plan of questionnaire have been made to test some participants knowledge about most security attacks terms to give most reliable estimate (neither over or under estimate) for knowledge that end users have about the two reasons.

2.1 Questionnaire

The questionnaire dividing the 50 participants into two main categories, high skilled and moderate computer users with knowledge.

The questionnaire built to test:

1- The understand the most security attacks that related to Online Payment System and most that attacks the end user computer system NOT the Server and Business side.
2- Test their knowledge of how to response if one of the attacks happen.
3- Their knowledge of using the proper tools against each type of attacks.
4- Concern on very popular attack "Anti Virus".
5- Their preferences of being only and make payments compared to browse online, make an orders and pay later (when good arrive to consumer's address).
6- The knowledge of managing the online banking transactions.

Clear definitions are submitted to participants related to the security terms such as:

1. social engineering
2. Phishing
3. Man-in-the-middle
4. Trojan horses
5. Fraud
6. scams
7. Key logger

3. RESULTS

The questionnaire submitted to 50 participants, but the only considered were 30 due to some anomalies in the rest of responses.

The responders classified into two categories, the first class whom consider themselves as computer specialists or having well knowledge for computer and internet users, while the second class classified as having moderate experience for computer and Internet applications especially the social media (Facebook and Instagram) without high skills of facing general attacks in case of facing them.

The results for the proposed questionnaire showed dramatically variant between the investigated two categories, high skilled end users have shown a good level of knowledge about the attacks (as expected), but the worse were they do not have any experience about how to response to the attack.

The results for the other category "users with moderate level of security knowledge" stated that there is a huge gab of experience the security attacks that related to Online Payment System.

As expected, the first class showed more knowledge for basic principles of computer security such as antiviruses while the fail to recognize other major attacks such as phishing, scam, and key loggers.

As the class one considered themselves having high level experience with computer and internet applications, the research expected them to have a good score of security attacks and the way they should to defend against them, unfortunately the results stated the opposite.

Graph 1 draw the figures in table 1 which clarify the unexpected poor knowledge for very essential attack which may they experience in future when start using the online payment system.

Table 1 End user knowledge about main security threats against electronic payment a system

Attack type	good	moderate	low	Never heard of it before
Phishing	0	3	5	22
Social Engineering	2	3	10	15
Man-in-the-middle	0	4	9	17
Trojan horses	5	7	10	8
Fraud	0	3	7	20
Key logger	7	9	7	7

DOI : 10.31695/IJERAT.2018.3311

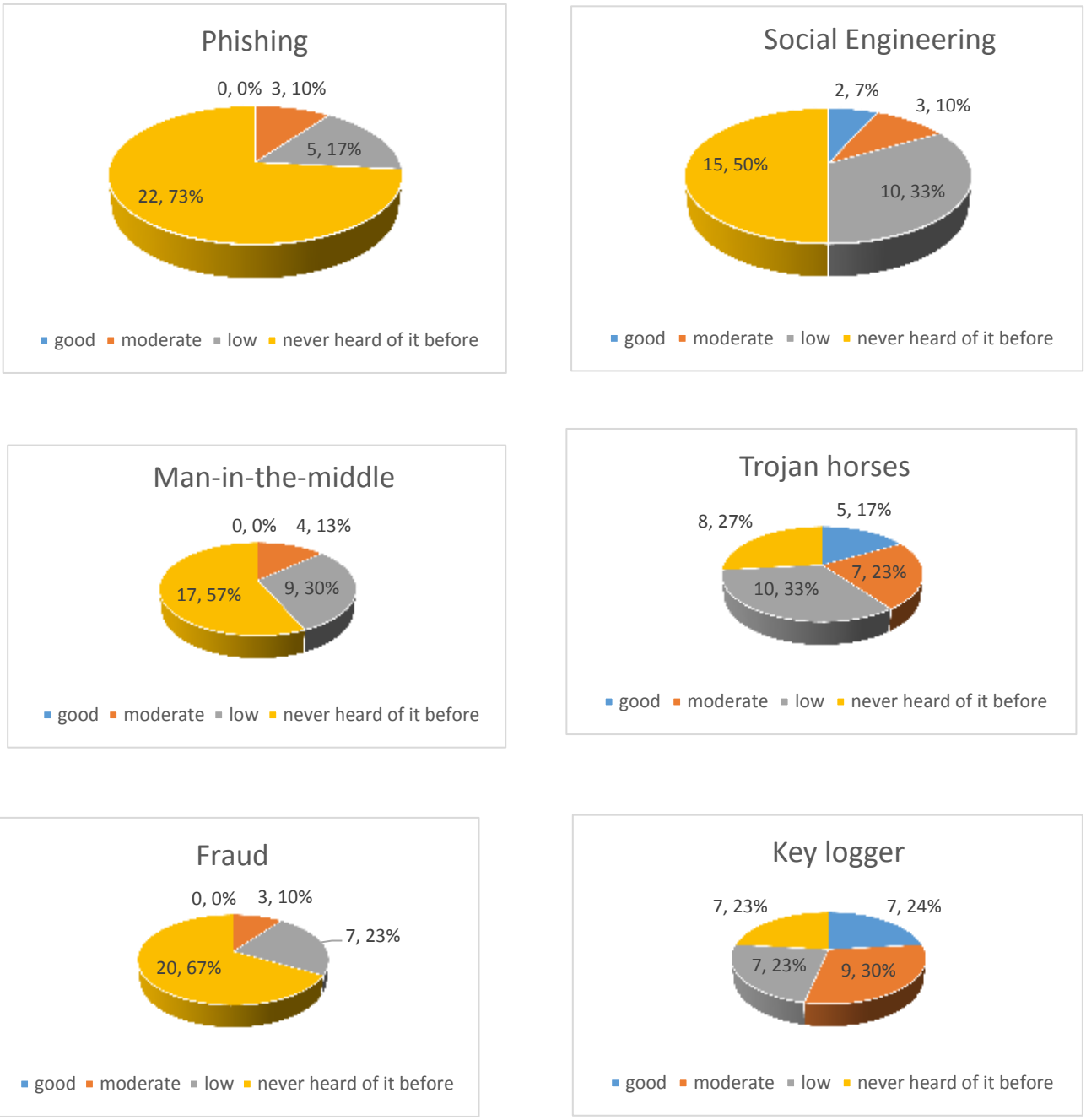

Figure 3 participants knowledge about major Security Threats against online transactions

4. CONCLUSIONS

The best conclusions can be gained from this research are:

1- Most applicant employees are not familiar with the security attack that may facing when start using the online payment system enforced by the government.
2- Security attack attempts will increase due the poor knowledge of basic possible techniques used by cyber attackers.
3- Loose of trust may appear between the client and the financial organization whom housing the electronic accounts for employed nor because the weak preparation made by the financial institutes but due to the low level for the clients themselves.

4.1 Recommendation

1- Financial institutes can design an acceptable security knowledge course to be provided to their client to increase the security awareness.
2- Academic studies in computer science must afford a high responsibility of increasing the security awareness regarding the new emerging technology (electronic payment system).
3- All other civilian organization have to participates in the educating the possible clients for the state of the art regarding the security attacks that facing the electronic payment system.

REFERENCES

1. al-Mahmood, H., & al-Khafaji, R. W. (2017, August). Protecting Recovery Information From Social Engineering Attack. *International Journal Of Modern Trends In Engineering And Research*.
2. HSBC. (2018). *Types of online attack.* HSBC Bank. Retrieved 06 13, 2018, from https://www.hsbc.com/online-banking/online-security/types-of-online-attack
3. Khrais, L. T. (2015, September 14). Highlighting the Vulnerabilities of Online Banking System. *Journal of Internet Banking and Commerce*. Retrieved 05 17, 2018, from http://www.icommercecentral.com/open-access/highlighting-the-vulnerabilities-of-online-banking-system.php?aid=61518
4. Miko, K. (2010, April 29). Internet Banking Attacks. *Slideshare*. Retrieved 06 07, 2018, from https://www.slideshare.net/DCIT/internet-banking-attacks-karel-miko
5. Wueest, C. (2017). *ISTR Financial Threats Review 2017.* Retrieved 06 1, 2018, from https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/istr-financial-threats-review-2017-en.pdf

DOI : 10.31695/IJERAT.2018.3311