Journal of Theoretical and Applied Information Technology
31st August 2022. Vol.100. No 16

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

ASSESSMENT OF CYBERSECURITY AWARENESS AMONG E-BANKING IN PALESTINE - EMPIRICAL STUDY FROM CUSTOMER'S PERSPECTIVE

DERAR ELEYAN[1] , RASHEED YOUSEF [2], AMNA ELEYAN[3]
[12]Faculty of Applied Science. Applied Computing Department,
Palestine Technical University-Kadoorie, Tulkarem- Palestine
[3] Department of Computing and Mathematics, Manchester Metropolitan University, United Kingdom
[1]d.eleyan@ptuk.edu.ps, [2]r.f.yousef1@students.ptuk.edu.ps,[3]a.eleyan@mmu.ac.uk

ABSTRACT

The internet services are available and widely expanded in Palestine. This expansion and availability contributed positively in enhancing the quality of services especially in E-banking. The internet services are enhanced and developed after the development and adoption of 3G/4G technology and infrastructure. This development widens the existing services and creates more opportunities for cybercrimes and security threats. These threats mainly attract the financial services. More and more users and beneficiaries become victims; therefore, more awareness is required amongst users and those involved in the e-banking services. In this study performed in depth analysis to measure the level of security and threats awareness related to E-banking service in Palestine and what are the main difficulties which faced the E-banking users in Palestine. Results showed that the average age of e-banking users and customers are from 30-40 years old are 42.4%, 65.3% of them are males and 55.4% holding BA degree as a level of education and 70% of the customers are using the e-banking services for more than a year. Recommendations have been suggested to raise the customers awareness to avoid victims and minimize the loss of data and money.

Keywords: *Cybersecurity, E-Banking, Cybercrime, Security Awareness.*

1. INTRODUCTION

Undoubtedly the growth of Internet worldwide facilitates the Life, creates more services and stratifies life needs like E-government, E-learning, E-shopping and E-banking, so people can use these services without a physical presence in the place where the services offer and to get the chance to achieve what they want from home and work via PC, laptops and mobile phones by using a customize application created for a certain function.

Online banking or E-banking can be defined as a secure access to the bank account and the relevant services through the bank website or mobile application. These services are expanded from check balances, pay bills, view transactions, transfer money locally and worldwide and many more services like order cheque book and ATM card. The E-banking services started first time in the USA during 1981, then reached to Europe [1],[2],[3]as a revelational service and that effects on the banking industry worldwide for retail and small value products.

According to (Juniper Research,2020) around two billion customers using the e-banking service worldwide via a range of smartphones, smartwatch and tablets and this number is increasing exponentially due to many factors such as the friendly user interface of the applications, time saving and low cost of these services, also the pandemic of Covid-19 effects on rapid increase of the users for these services since they cannot visit the bank to do financial transactions. And this applies, respectively to the users of these services in Palestine.

Utilising online banking services involves risks related to cybersecurity issue, online banking services are attractive to the Cybercrime offender because it contains many sensitive data the offender may use for fraud or electronic blackmail or even unauthorized financial transfers, So the security became the main concern for the e-banking users and all the banks which offer such services. They exert every effort to provide security to the users of these services and improve trust and confidence.

Online banking brings many benefits to the banking industry but on the other hand it creates a

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

significate opportunity for the Cybercrime offenders. The first case of cyber fraud has been reported in 2004[4] .The cybercrime against the financial institutions increased by more than 30% between 2015 and 2017 [5], and its 300 times more frequently than the other sectors [6] where the estimated value of the annual global cost of cybercrime against the banking around 100 $ billion [7], and for the Middle East the estimated value will be around 25 $ billion for the upcoming 10 years [7].

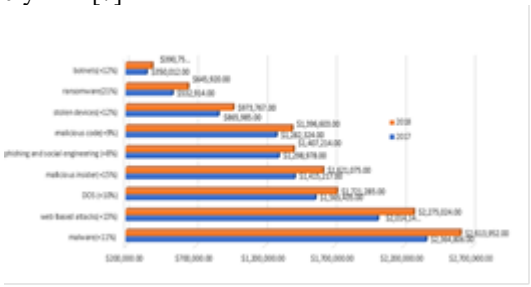

Figure1. Average Annual Cost Of Cybercrime By Type Of Attack In 2017 And 2018 According To A Report Of Ponemon Institute And Accenture (2019

2. E-BANKING IN PALESTINE

In the last 10 years, the growth of Internet penetration in Palestine increased rapidly, according to the Palestinian Central Bureau of Statistics, Internet Penetration increased from 64.5% in 2018 to 72.3 % in 2019. And the average percentage of individuals (10 Years and above) who use the Internet and exposed to informatics threats on the Internet in Palestine by region in 2019 was around 4.2% such as Manipulation of digital documents, Fraud, and Identity theft (personal identification number, Passport, Password for financial and non-financial accounts.

Referring to the reports of the Electronic Crime Unit in Palestine, the cybercrime cases increased every year especially the cases which related to the financial fraud. In general, the unit dealt with 2568 cases in 2018 and it increased by 26.6% from 2017, and 667 cases were related to financial fraud.

The online banking services started first time in the Palestinian market during 2007 and 2008 and services now available in local and expatriate banks (PMA ,2021). Now in Palestine we have 7 local banks and 6 Expatriate banks all of them offer all kinds of e-banking and e-payments services which includes managing accounts, paying bills for many services' provider, transfer money between accounts or other banks, request a specific service such as ATM card or ChequeBook and many other services.

Banks in Palestine have an annual budget to enhance the security of the e-banking services between 150,000$ - 500,000$ every year depends on the size of the bank and the sorts of cyber-security method and vendor.

Based on many reports of Palestine Monetary Authority, Palestine Capital Market Authority and Palestine Economic Policy Research Institute during 2016 and 2017: 36.4 % of the Population in Palestine have active accounts and less than 6.4 % of them use the e-banking. One of the main issues which they mentioned in the reports that the users still do not trust these services and they preferred to stay away from offered services and channels.

3. LITERATURE REVIEW

Over the last 15 years many researches bring out the importance of the security in all services and channels which use the Internet and are focused on various topics about the cybersecurity issues. [8] measured users level of awareness for cybersecurity tips when they were using the E-banking also measured the effect of socio-economic factors on the level of awareness for cyber security Tips when they are using the E-banking by using a sample of 200 bank customers .The results showed that the majority of customers were well exposed to cyber threats and cybercrime also they found that socio-economic factor plays a vital role in the driving the level of awareness of customer for cybersecurity threats. 2021 Cybersecurity statistics shows that 98% of cyber-attacks were perpetrated by attackers relying on social engineering and 43% of IT professionals were victims of such attacks in the previous year. In addition to the fact that new employees. [18].

Another study [9] analyzed the customers perceptions and awareness about E-banking security also understood the problems which the customers faced while using e-banking services by using a sample of 50 customers from one region. The study found that only 32% of the respondents were aware of the security issues in E-banking and 50% of the respondents faced cyber-attack such as hacking and phishing attacks. This study, also focused on the lack of knowledge on the victims of cyber-crime also the role of the local government and banks to do Awareness campaigns about the cyber security threats. [10] tested the hypothesis of

the educational level of the respondents and its effects on their level of awareness on phishing attacks. Also, the hypothesis of the rate at which respondent's information has been breached while E-banking effects by the level of awareness on viruses and malware attacks. This study conducted a survey about 5 common cyber security threats, the authors found that the majority of respondents thought that the E-banking is safe and secure and therefor they don't aware of security risks associated with online banking and the level of education did not fill the gap of information security awareness. Therefore, they proposed methods of awareness to fill this gab like Television and radio advertisement, also quarterly seminars can improve the customers knowledge about security risks.

[4]concluded that in order to reduce the security risks of E-banking it's important to initiate awareness and knowledge of the customers and this action should be done by collaboration between the government and the private sectors.

[11] used questionnaire and interview on a sample of banks customers in Bangladesh, the research discussed the reasons of not choosing E-banking services, they found that 55.74 % of the sample have no idea about the security and 9.84% of them avoided this service due to security issues and the lack of technologies knowledge. In the end of the study the authors concluded that several "Security breaching" events in the banking sector of Bangladesh made people confused.so, both the government and the banks should come forward to providing knowledge about the security risk which related to these services and that can improve the usability and reduce the number of users in addition to protect them from such risks.

4. FORMS OF ATTACKS ON E-BANKING AND THEIR PREVENTIONS MEASUREMENT

The cyber criminals developing every day sophisticated ways the users of the E-banking users to seal the financial information such as password, accounts number, and identity credit card numbers, the effects of stealing such information will be fatal on the end user, on other hand the E-banking carried out new tools since the financial information will be more attractive for the attacker, below are a summary of the common threats to E-banking [3],[7],[10],[13],[14],[15],[16],[17]:

- Malware: malicious software variants, including viruses, ransomware and spyware. Shorthand for malicious software, malware typically consists of code developed by cyberattacks, designed to cause extensive damage to data and systems or to gain unauthorized access to combinational information and data sources, the users of E-banking can be a victim of malware by downloading untrusted application or by clicking unnecessary links. The users of E-banking can prevent such threats by avoid following untrusted links and having antivirus software on their PC, Laptop and mobile. In addition to keep scanning the devices which connected to E-banking applications and websites and by avoid download crack software which may have Trojans that can steal confidential information.

- Social engineering: this kind of threats based on manipulating people so they give up confidential information[16]. The types of information these criminals are seeking can vary, but when individuals are targeted, the criminals are usually trying to trick into giving them your passwords or bank information, or get access to your computer then secretly install malicious software–that will give them access to passwords and bank information as well as giving them control over computer and confidential information. The users can avoid this kind of threats by not sharing username and password with any one also by avoiding surfing the untrusted website which may contains Trojans or malware.

- Phishing: it's a kind of social engineering attack the offender sent an E-mail or text message to the victim with attractive text to click the links which included in the body of the mail or message which can lead to the installation of malware, the freezing of the system as part of a ransomware attack or the revealing of sensitive information[16]. The user can avoid the phishing threats by keeping the brewers up to date and by using antivirus software, also not clicking on suspicious links will help the user to avoid such a threat.

- Identity Theft: this threat occurs when the offender uses the personal information of someone else like name or credit card

number without their permission, to commit fraud or other crimes. To avoid identity theft online the users of E-banking should protect their devices (PC, laptop and smartphone) with strong, up-to-date security software and not to share their confidential information with anyone, also using strong password and not to use the same password everywhere.

- Keylogger: this kind of threats known as one of the oldest forms of malware. It's still popular and often used as part of larger cyber-attacks. Simply we can define it as a type of monitoring software designed to record keystrokes which made by a user. These keystroke loggers record the information you type into a website or application and send it back to a third party.

- Man-in-the-middle (MitM): this threat occurs when an attacker intercepts communication between the sender and receiver either to secretly eavesdrop or modify traffic traveling between the two. Attackers might use MitM attacks to steal login credentials or personal information. The users can avoid (MitM) by using two-factor authentication and not use public networks.

- Shoulder surfing: is a type of social engineering threats used to obtain information such as (PINs), passwords and other confidential data by looking over the victim's shoulder. The offender can watch the keystrokes inputted on a device or listen to sensitive information being spoken. The users can avoid this kind of threats by pick strong passwords so it's hard for any observer to guess what the user type also not to use the E-banking services in public places.

- DOS Attack: denial-of-service attack is meant to shut down the service or network, making it inaccessible to its intended users. DoS attacks accomplish this by flooding the target with traffic or sending information that triggers a crash. The protection against DOS attack is the banks responsibility by developing a Denial-of-Service response plan, secure bank network infrastructure and using the cloud services since it has more bandwidth, and resources than the private network [15]

- Vishing: it is a social engineering attack that attempts to trick victims into giving up combinational information by the phone. Usually, the offender strategically manipulates human emotions, such as fear, sympathy, and greed in order to achieve their goals. Simply the users can avoid vishing calls by using one rule "call center won't call you to request that you to share or to change logins, passwords, or network settings. Any caller who makes this type of request is probably is cybercriminal and should refuse the request and notify your service provider".

[19] stated different type of credit card fraud detection techniques as decision trees, logistic regression, artificial neural networks, k-nearest neighborhood and K-means clustering.

5. RESEARCH METHODLOGY:

5.1 Research approach:

This study mainly based on primary sources conducted by questionnaire and partially based on other sources such as reports which publish by official authorities. Secondary data source included journals, internet reports, etc. This research originates from the question of if E-banking customers in Palestine fully aware of the cyber security threats and risks which related to cybercrime? So, to address this question, a set of questionnaires were developed to answer the research questions and meet the objectives.

Figure 2 summarize the secondary data source the research approach- PRISMA flow diagram. Presentation of the procedure of literature searching and selection with numbers of articles at each stage

Data are collected from the respondents through an online survey. SPSS (Statistical Package for the Social Sciences) tool was applied to analyze and test the model.

Figure 2 summarize the secondary data source the research approach- PRISMA flow diagram. Presentation of the procedure of literature searching and selection with numbers of articles at each stage.

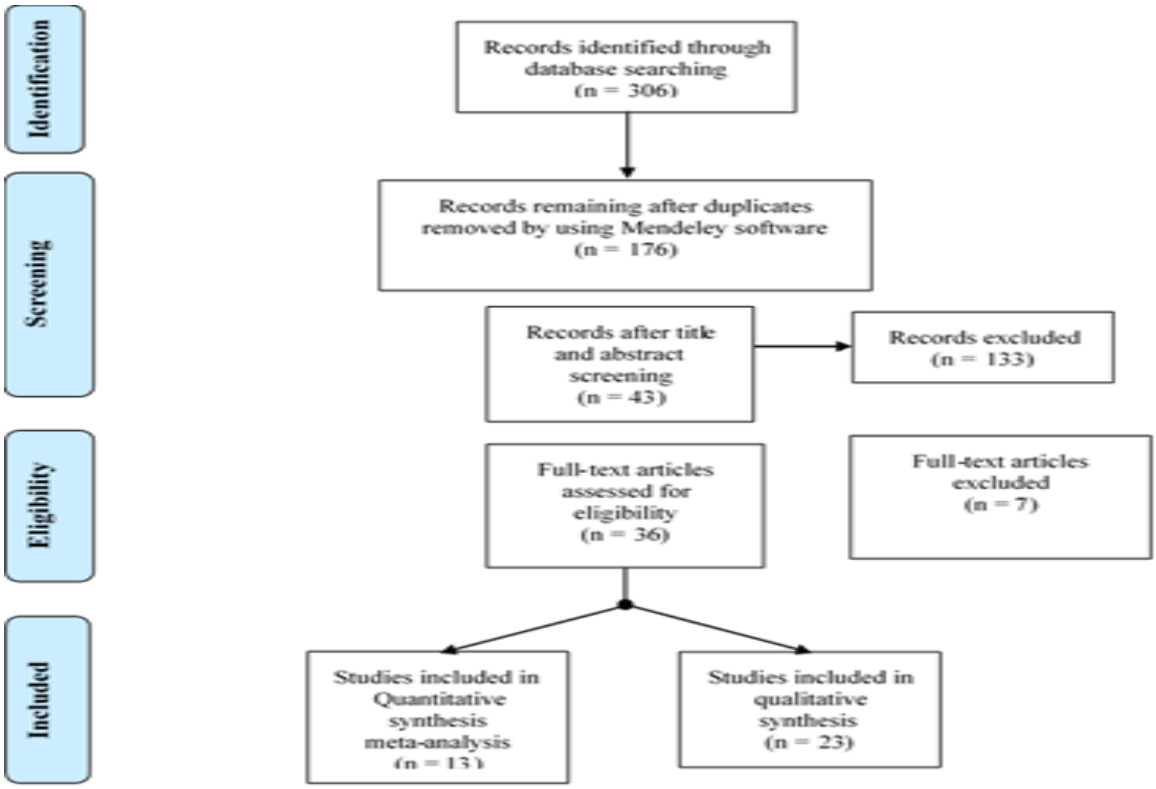

Figure 2: PRISMA flow diagram

5.2 *Study Location :* the geographical scope or the study location of the present research work was West Bank & Gaza, and the respondents were of local and expatriate banks operating in the district area.

5.3 *Sample size :* this study a used google questionnaire, the number of respondents was 204, 97% of the respondents have an active bank account and 73.5 % of them using E-banking services .

5.4 *Data collection method :*As we mentioned above, we used google questionnaire form we have used two ways: the first one is to distribute the form through Internet randomly to get response from random people.The second way to get permission from two local banks to make the four customer services in four different locations to ask the bank customers in the branch the questions which included in the questionnaire form and it filled by the customer services employees.

6 STUDY DESIGN:

The hypotheses of the study are the following:

H_{01}: The customers of E-banking In Palestine fully aware about the security awareness which related to these services.

H_{02}: The education level of the respondents does not influence their level of awareness for security risks which related to E-banking services.

This study focused on the following questions that are addressed on the questionnaire:

1- Are E-banking customers in Palestine fully aware of the cyber security threats and risks which related to cybercrime?
2- Do the factors of education level and age influence the customer's awareness about security threats?
3- What is the Impact of E-banking security among the selected customers in Palestine?
4- What are the major problems faced by the customers while using the E-banking services in Palestine?
5- Does the factor of socio-economic effects of the level of awareness of cyber security among E-banking users?
6- What do the other regions do to improve the customer's awareness which related to the E-banking security threats?

Journal of Theoretical and Applied Information Technology
31st August 2022. Vol.100. No 16

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

7 DATA ANALYSIS AND INTERPRETATIONS:

In this section. we will highlight the main finding of the questionnaire also highlighting the main characteristics of the result.

- Age average of respondents:

As we can see in Table 1 below the result of respondents age category:

Table 1. Age category of the respondents.

Age category	Percentage
20-30	15.3%
30-40	42.4%
40-50	24.6%
Above 50 years	17.7%

- Gender of the respondents:

Table 2 shows the percentage of female and male whom they participated in the study questionnaire:

Table 2. gender of the respondents.

Age category	Percentage
Female	34.3%
Male	65.3%

- Educational level of the respondents:

Table 3 shows the percentage of educational level category for the respondents:

Table 3. Educational level category of the respondents.

Educational level category	Percentage
Less than matriculation	8.8%
Matriculation	15.2%
B. A	55.4%
Post Graduate	20.6%

- E-banking serveries Penetration, and the percentage of E-banking users of the respondents

As a result of this study, we have found that 73.5% of the respondents are using E-banking services, the Table 4 shows the how long they are using the E-banking services:

Table 4. how long the respondents using the E-banking services.

Period of Using E-banking category	Percentage
Less than one month	2.6%
1-6 months	11.2%
6-12 months	9.6%
More than one year	70%

- Reasons for using E-banking service from the respondent's point of view: the figure *3* shows the percentage of each reason:

A. The availability of the services: E-banking is 24X7 services the user can access to it anytime and anywhere.
B. Better prices for the services against the onsite services.
C. Information security.
D. .Better exchange rate.
E. Easy to use and to keep up to date with accounts information

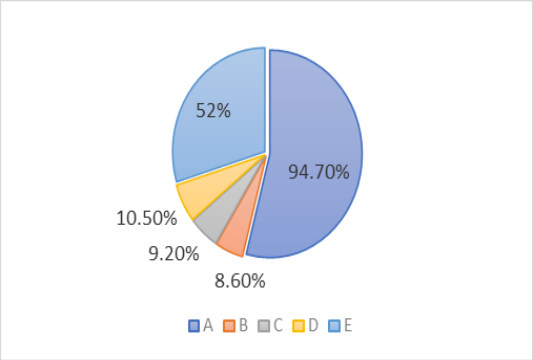

Figure 3 : reasons of using E-banking service from the respondent's point of view

- The difficulties which faced the E-banking users in Palestine: the figure 5 shows the percentage of each difficulty:

A. It's too difficult to remember the user's name and the password.
B. Reliability on the Internet service.
C. Limited services.
D. Issues related to the Information security.
E. Lack of help from bank employees regarding to the E-banking services.
F. There are no difficulties.

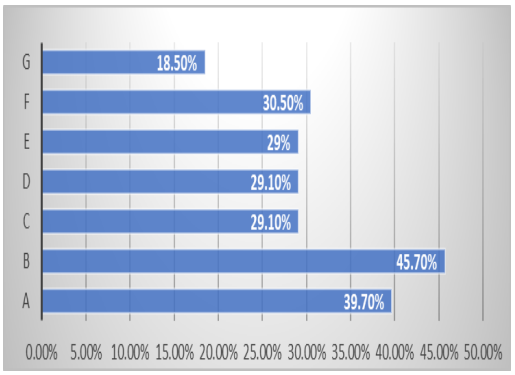

Figure 5: The Difficulties Which Faced The E-Banking Users In Palestine

- Types of services which respondents Benefit from using the E-banking services: the figure 4 shows the percentage of each type of service:

A. Calculate payments of the loans.
B. Get loan and Banking facilities applications.
C. Check accounts statements.
D. Apply for loans or Banking facilities.
E. Transfer between accounts within same account or other account in the same bank.
F. E-payment services.
G. Other kind of services.

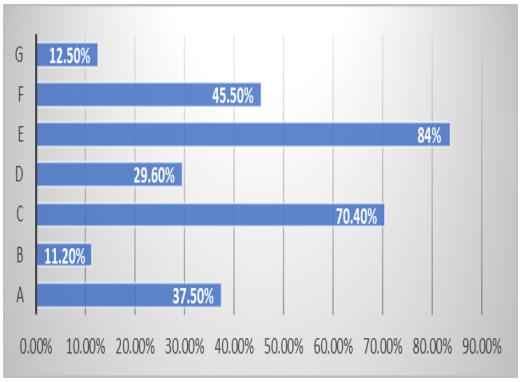

Figure 4: Percentage Of Service Which Respondents Benefit From Using The E-Banking Services

- Do the E-banking customers in Palestine trust the services: Table 5 shows the answers of the respondents when we ask them if they trust the E-banking services:

Table 5. Do The Respondents Trust E-Banking Services?

Do you trust E-banking services?	Percentage
I totally trust it	21.7%
Kind of yes	58.6%
doubtable	11.8%
I don't trust it	20.6%

- Do the E-banking customers in Palestine think that the E-banking service of them banks is secure: when we asked the respondents of the questionnaire about if they think that the E-banking service of them banks is secure, we have got the answers as table *6*.

Table 7. Do The E-Banking Customers In Palestine Aware Of The Security Threats Facing Internet Banking Services

Do you trust E-banking services?	Percentage
Yes	36.2%
No	35.5%
Maybe	28.3%

- Do the E-banking customers in Palestine aware of the security threats facing Internet Banking services: Table 7 summarize the answers of respondents about if they aware of the security threats facing Internet Banking services:

Table 7. Do The E-Banking Customers In Palestine Aware Of The Security Threats Facing Internet Banking Services

Do E-banking customers Palestine aware of the security threats facing Internet Banking services?	Percentage
I do not know that there are threats related to information security and I don't Aware of these threats	26.5%
I'm aware about the threats related to information security, but not all kind of it.	57.4%
I'm aware about all kinds of threats	16.1%

- How did the E-banking customers in Palestine hear about the security threats facing internet banking services: Table *8* shown the answers of the respondents when we ask them How did you hear about the security threats facing internet banking services?

Table 8. Do The E-Banking Customers In Palestine Aware Of The Security Threats Facing Internet Banking Services

How did you hear about the security threats facing internet banking services?	Percentage
Radio and television stations and government media	1.9%
awareness messages from your bank	33.5%
Social media	45.2%
I never heard about it	19.4%

- Do the E-banking customers in Palestine still visiting the bank – physically although they activated the E-banking: Table *9* summarize the answers of respondents about if they still physically visiting the bank –although they activated the E-banking

Table 9. Result Of The Question If They Still Physically Visiting The Bank –Although They Activated The E-Banking.

Have you ever visited the bank branch since they started using Internet banking?	Percentage
Yes	78.9%
No	21.1%

8 RESULT DISCUSSION:

After reviewing and analysis the result which talked about in the above section, we need now to apply these results to the main Hypothesis of this study:

H 01: The customers of E-banking in Palestine fully aware about the security awareness which related to these services.

Back to the results of the question if do E-banking customers Palestine aware of the security threats facing Internet Banking services? We have found 26.5% (41 respondents) of the respondents which were 154 persons for this question they did not know that there are threats related to information security and they are not aware of these threats and 57.4% of the respondents (89 respondents) aware about the threats related to information security, but not all kind of it.

Also, during the analysis about the question of How did you hear about the security threats facing Internet banking services, we have found that 19.4% (30 respondents out of 155 respondents) they never heard about the security threats facing internet banking services. so based on the result which mentioned above the H 01 is accepted the customers of E-banking in Palestine fully aware about the security awareness which related to these services.

H02: The education level of the respondents does not influence their level of awareness for security risks which related to E-banking services: According to this hypothesis we have we tried to connect different Educational level category of the all respondents of all the sections of the questionnaire (204 respondents) which is shown in Table3 , with the results which found in table 7and 8 are the core of this study , and we have noticed that most of the answers which related to the respondents with education level of less than matriculation are negative about the aware of security threats (average of positive answers is 4.7%) however the answers of the respondent with matriculation B.A degree (144 respondents) the average of positive answers is around 57.9%. One the other hand, we have examined the average of positive answers in the educational level category of high education (42 respondents) and we found that the average is 81.6%.

So, the H 02 is not accepted the education level of the respondents influence their level of awareness for security risks that are related to E-banking services.

H03: The age of the respondents does not influence their level of awareness for security risks which related to E-banking services: According to this hypothesis we have we tried to connect

different age category of the all respondents of all the sections of the questionnaire (204 respondents) which shown in Table1 .The results which are found in Tables 6 and 7 are the core of this study this study and we have noticed that the age categories of 50 years and above has a low average of positive answers about the awareness of security threats which was only 9.8% while the average of for the Age category 30-40 was 48.1% and for the Age category 40-50 was 36.3% , also we have found the average of positives answers for Age category of 20-30 was 22.6% .

So, the H 03 is not accepted and the age of the respondents influence their level of awareness for security risks which related to E-banking services – it's normal average for 30-40 and 40-50, but its low for the Age category of 20-30 and 50 years and above.

Other result should be highlight and recommendations should be considered:

- The role of government: We have noticed that the role of government is not observed as we noticed during the analysis of result of the question of" How did you hear about the security threats facing internet banking services?" only 1.9% of the respondents heard about the security threats facing internet banking services (3 respondents only) via the Radio, Tv and governments, and this is a very low average.

The recommendation: the government in Palestine should have a major role to pay attention to the security threats in general and security threats facing internet banking services, the ministry of telecommunication and information technology In cooperation with the Cyber Crime Unit should issue periodically about the cybercrime and security threats via Radio, TV also using the social network to pay more attention about these things. The periodical or advertisement should be directed to different age groups with easy language to ensure that it will effective for different ages and educational levels.

- The major role of social network: as we noticed during the analysis the result the question" How did you hear about the security threats facing internet banking services?" 45.2% of the respondent answered that they heard about it via the social network. Here, the great role of social media appears in order to pay attention to the security threats facing internet banking services.

The recommendation: government and banks should take advantage of this great role of social network in order to warn users of the risks of security threats facing Internet banking services and the negative consequences that may occur if they are exposed to these threats.

- The difficulties which faced the E-banking users in Palestine: we have noticed that there are four main difficulties which faced the E-banking users in Palestine:

1. Limited services: 29.1 % of E-banking users that were responded to our questionnaire choose this option as a difficulty which faced the E-banking user.
2. Reliability on the Internet service: 45.7 % of E-banking users which responded to our questionnaire choose this option as a difficulty which faced the E-banking user.
3. It's too difficult to remember the user's name and the password: 39.7% of E-banking users which responded to our questionnaire choose this option as a difficulty which faced the E-banking user.
4. Lack of help from bank employees regarding to the E-banking services: 30.5 % of E-banking users which responded to our questionnaire choose this option as a difficulty which faced the E-banking user.

The recommendation: according to the limited services with the E-banking application the banks should do more work to improve the services which should available on E-banking applications based on the actual needs of the users by sending feedback requests to the users or doing quick interviews in the branches with the customers by qualified employees.

For the issues which related to Reliability on the Internet service banks should work with mobile phone companies to provide the users with free access to the application of E-banking via 3G/4G networks and this features already offered in other countries.

Regarding the password issues the banks worldwide now is working to enhance their application with biometric access such as fingerprint and face recognition feature, by using these features, the passwords topic will not become a major obstacle for users.

And last but not least, Banks should employ more methods to train new and existing E-banking users about the application or web site itself, and this can be done by developing plug -in software to guide the users while using the application or tutorial videos installed with the application or available on the web site which provide E-banking services directed to different age groups with easy language to ensure that it will effective for different ages and educational levels.

5 CONCLUSION AND FUTURE WORK :

To sum up, this study analyzed the Internet banking customers in Palestine to understand various aspects of Internet banking services, and the concerns on security measures by consumers. This study focused on the relation between the educational level and age with the level of awareness for security risks which related to E-banking services based on two hypotheses and we have that the two factors influence on the level of awareness for security risks which related to E-banking services. In addition, we focused on the role of the Palestinian government through the specialized ministries in order to participate in a bigger role to pay more attention to risks of cyber threats related to E-banking services since the user of these services are not fully aware of it as we have found.

For the future work, we should focus on the E-payment channels which began to spread widely in the past two years, and the security awareness according to these services still not mature Where the damage could be destructive.

9 ACKNOWLEDGMENTS:

We gratefully thank Palestine Technical University-Kadoorie for support this study.
And we also gratefully thank Palestine monetary authority, Palestinian Central Bureau of Statistics, Palestine Capital Market Authority and cybercrime unit- Palestine Police for the support and facilitating the access to the statistics and data .

REFERENCES:

[1] J. Jayaram and P. Prasad, "Review of E-banking System and Exploring the Research Gap in Indian Banking Context," Int. J. Innov. Res. …, vol. 2, no. 2, pp. 407–417, 2013, [Online]. Available: http://ijird.com/index.php/ijird/article/view/581.

[2] T. R. Ou and L. A. C. Omplete, "LA BANQUE TRADITIONNELLE OU LA COMPLETE-T-IL," Université de Liège, 2008.

[3] "Risk Management For Electronic Banking And Electronic Money Activities," 2003. [Online]. Available: http://www.bis.org/publ/bcbs98.htm.

[4] M. Tabiaa, A. Madani, and N. El Kamoun, "E-Banking: Security risks, previsions and recommendations," IJCSNS Int. J. Comput. Sci. Netw. Secur., vol. 17, no. 11, pp. 189–196, 2017.

[5] O. Akanle, J. O. Adesina, and E. P. Akarah, "Towards human dignity and the internet: The cybercrime (yahoo yahoo) phenomenon in Nigeria," African J. Sci. Technol. Innov. Dev., vol. 8, no. 2, pp. 213–220, 2016, doi: 10.1080/20421338.2016.1147209.

[6] V. Wang, H. Nnaji, and J. Jung, "Internet banking in Nigeria: Cyber security breaches, practices and capability," Int. J. Law, Crime Justice, vol. 62, no. May, p. 100415, 2020, doi: 10.1016/j.ijlcj.2020.100415.

[7] L. Ali, F. Ali, P. Surendran, and B. Thomas, "The Effects of Cyber Threats on Customer's Behaviour in e-Banking Services," Int. J. e-Education, e-Business, e-Management e-Learning, vol. 7, no. 1, pp. 70–78, 2017, doi: 10.17706/ijeeee.2017.7.1.70-78.

[8] A. Adholiya and S. Adholiya, "A Study on Cyber Security Practices and Tips Awareness among E- Banking A Study on Cyber Security Practices and Tips Awareness among E-Banking Services Users of Udaipur , Rajasthan," Int. J. Sci. Res. Multidiscip. Study, vol. 5, no. 8, pp. 148–154, 2019.

[9] V. Vimala, "An Evaluative Study on Internet Banking Security among Selected Indian Bank Customers," Amity J. Manag. Res., vol. 1, no. 1, pp. 63–79, 2016.

[10] M. Olalere, V. O. Waziri, I. Ismaila, O. S. Adebayo, and O. Ololade, "Assessment of Information Security Awareness among Online Banking Costumers in Nigeria," vol. 4, no. 6, pp. 13–24, 2014.

[11] B. F. K, S. A. Chowdhury, A. Haque, S. Akter, S. Muhammad, and H. Ahsan, "E-Banking Adoption in Bangladesh; Present Status and Customer Satisfaction: An Evaluationt," vol. 21, no. 1, 2021.

[12] P. Subsorn and S. Limwiriyakul, "A Comparative analysis of internet banking security in Thailand: A customer perspective," Procedia Eng., vol. 32, pp. 260–272, 2012, doi: 10.1016/j.proeng.2012.01.1266.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[13] A. Mishra, A. Awal, J. Elijah, and I. Rabiu, "An Assessment of the Level of Information Security Awareness among Online Banking Users in Nigeria," Int. J. Comput. Sci. Mob. Comput., vol. 6, no. 5, pp. 373–387, 2017, [Online]. Available: www.ijcsmc.com.

[14] B. Chaimaa, E. Najib, and H. Rachid, "E-banking Overview: Concepts, Challenges and Solutions," Wirel. Pers. Commun., no. October, 2020, doi: 10.1007/s11277-020-07911-0.

[15] R. Khader and D. Eleyan, "Survey of DoS/DDoS attacks in IoT," Sustain. Eng. Innov., vol. 3, no. 1, pp. 23–28, 2021, doi: 10.37868/sei.v3i1.124.

[16] A. Naser, M. Jazzar, D. Eleyan, and A. Eleyan, "Social Engineering Attacks : A Phishing Case Simulation," no. 03, 2021.

[17] J. Jansen and R. Leukfeldt, "Phishing and malware attacks on online banking customers in the Netherlands: A qualitative analysis of factors leading to victimization," Int. J. Cyber Criminol., vol. 10, no. 1, pp. 79–91, 2016, doi: 10.5281/zenodo.58523.

[18] Odeh, N., Eleyan, D., Eleyan, A., " A Survey of Social Engineering Attacks : Detection and Prevention Tools" , Journal of Theoritical and Applied Information Technology, Vol. 99, No. 18, pp. 4375-4386,September, 2021.

[19] Fayyomi, A., Eleyan, D., Eleyan, A., "Asurvey paper on Credit Card Fraud Detection Techniques",Vol. 10, Issue 9, September 2021.