ISSN 2278-3091
Volume 10, No.2, March - April 2021
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse471022021.pdf
https://doi.org/10.30534/ijatcse/2021/471022021

The Impact of Phishing on the Business Sector in KSA : Analytical Study

Hanin Younis Esmat[1], Alaa Faisal Alharbi[2], Abdelrahman Karrar[3]
[1]Information System Department , Taibah University, KSA , tu4160208@taibahu.edu.sa
[2]Information System Department , Taibah University, KSA, tu4160217@taibahu.edu.sa
[3]College of Computer Science and Engineering, Taibah University, KSA, akarrar@taibahu.edu.sa

ABSTRACT

One of an old topic that has been sparked controversy and debate since the beginning of the development of the Internet and the emergence of sites is talking about the privacy and confidentiality of user information on the Internet, and today the software or technologies that record user behaviour in a site with the aim of collecting marketing information about users and selling them later to companies and economic institutions, is considered undesirable with it, but we are still generally on the safe side. The paper describes theft operations known as Phishing, electronic phishing, or electronic fraud that may cost you all of your savings. Phishing is a criminal activity that uses the method of social engineering and is one of the most effective ways to trick people who pay little attention. Many hackers use hidden methods such as malware infecting the user devices to steal your sensitive information, while some of the professionals directly request the details, depending on the lack of user experience. This paper will attract the interest of everyone working in the government or private sector. Additionally, it will be very beneficial for the business sector, especially staff dealing with outside parties.

Key words: Phishing, Cybercrime, Malware, Suspicious e-mail, Identity theft, Financial theft, Accellion, Security Awareness.

I. INTRODUCTION

Phishing is one of the most common types of cybercrime. Electronic phishing is a method of online fraud, in an attempt to obtain personal or financial information such as username, password, and credit card details of individuals through e-mail messages or through websites used to gain a foothold in the organization & business sector's network as a part of a large attack [1][2].

An organization under such an attack usually tolerate financial losses in addition to low market share, reputation, and a lack of consumer confidence. Depending on the scope, the phishing attempt may escalate into a security incident that makes it difficult for the business to recover.

A phishing kit is the web component, usually an e-mail and objects to get the user to do something. Most phishing kits are stored on a compromised web server or website and usually remain live for 36 hours before they are detected and removed [3].

One of the oldest types of cyber-attacks is the first reason to choose this kind of cybersecurity that dates back to the 1990s. It is still one of the most common and dangerous ways, as communications and manipulation techniques have become more advanced [4]. The second reason is facing difficulties to do our job in a proper way as employees in private and government sectors due to blocking send and receive external e-mails and browsing worldwide internet.

A common type of phishing scam attempt:

- Spoofed e-mail ostensibly.
- The e-mail claims that the user's password is about to expire [4].

This research paper will start by the introduction to identify Phishing methods and common types of the phishing scam. Then, it will discuss previous research paper and studies, which is about Phishing E-mail, user behaviour using learning tools, and some of phishing problems, and suggested solutions. The paper will also discuss the survey that conducted to measure the awareness level of the people and most familiar kind of phishing and how they usually act to avoid being a victim. Moreover, it will provide the solutions that real organizations and the business sector used to avoid phishing, the awareness level of the people. At the end of this research, it will conclude by a summary of this research paper, recommendations, our opinion of this kind of solutions and, Future work suggested for next research.

II. LITERATURE REVIEW

We are going to display the previous research papers and studies which is about An Analysis of User Behaviors in Phishing Mail using Machine Learning Technique written by Yi Li 1 ; KaiqiXiong 1 and Xiangyang Li in Proceedings of the 16th International Joint Conference on e-Business and Telecommunications (ICETE 2019) [5]. The second paper about Analysis of the Phishing Email Problem and Discussion of Possible Solutions that had been written by Christine Drake, Andrew Klein, Jonathan Oliver [6].

A. An analysis of user behaviours in phishing e-mail using machine learning techniques

This study aims to understand how user behaviours and phishing attacks relate, as cyber-attacks are of different degrees for each user depending on the levels of network security education. The research paper has shown that online fraud and user's acts are directly correlated to each other. One important security safeguard is to educate users by analyzing the results of the survey collected as the second step is to develop a model to predict the probability of how the user is going to be a victim.

On-site and online study has been proposing as study designs. The purpose of this research is to analyze the most malicious types of a phishing attack; there are three types of phishing:

- A Suspicious Sender's E-mail Address
- Suspicious Links or Attachments
- Malicious E-mail Contents

A survey had been created online to collect data (participants' answers). The survey contains 30 different questions related to the background of the participants, such as age, experience, and habits of using social media. This survey helps to understand user behavior related to phishing attacks.

Statistical methods have been applied to analyze the site's data set and explore answers to questions about types of deception and monetary incentives and how to interfere with behaviors. The machine learning method has also been developed as it helps to predict the probability of user performance in connection with phishing attacks and whether the user can perform it in the right way or not.

In conclusion, the analysis of the research paper shows that the performance of participants with intervention and a monetary incentive is better than the other participants that do not have any of these specifications. Besides, it was rating the suspicious senders' e-mail addresses as the most harmful phishing type to the users.

At the end of this paper, the researchers are planning to study more about the user behaviour that will be affected by multitasking and how it will be affected.

B. Analysis of the phishing email problem and discussion of possible solutions inputs

The scientific paper discussed the most common electronic fraud via e-mail and attempts to trick businesses and steal important data of users by denying the thief or fraudster as a trusted official entity to link relationships with the victim and gain the confidence to technically access the login credentials and obtain personal or financial information. It also harms electronic commerce, as this leads to a loss of confidence in Internet transactions. The paper discusses some of the results and reasons that lead people to fall into fraudulent e-mail messages. Then review some possible solutions for phishing.

A survey consisting of five e-mails was conducted and divided equally into legitimate and fraudulent e-mails, and the survey participants were classified by age, gender, family income, and employment status. Participants were asked to rate each e-mail whether fraudulent or legitimate. The results showed that participants mistakenly identified e-mails by 28 percent; 30 percent of respondents identified fraudulent e-mails as legitimate, and 19 percent of those defined legitimate e-mails as fraudulent. It also turned out that the younger age group was more likely to believe that the e-mails were legitimate while the older ones were warier and suspicious. E-mails have become more sophisticated and have started to appear in several languages , including Spanish, French, German, and Dutch.

One of the fraudulent techniques is to use psychological methods to manipulate victims and access information. For example, an e-mail is sent containing company data as it is on its webpage, such as it contains the company logo, the same font, and colour, so the recipient thinks it is a reliable message and falls into the trap. Some of them claim that the company needs to install new security software, so the recipient must update its data.

Results of the survey show that well-designed fraudulent e-mails can cheat large numbers of people.

Some of the economic losses resulting from phishing have been estimated in 2003 and 2004. The error in defining legitimate e-mail as fraud is devastating because it affects the Internet business; some people think that using Internet banking service is riskier despite the availability of security than paper or postal system. Finally, the paper discusses some phishing solutions:

1) Technical solutions

Technologies include phishing blacklists, encryption, authentication, URL abuse detection, and content filtering. In addition, some methods help to identify phishing e-mail messages as fraudulent and to allow them to access incoming mail and called encryption-based technology. Some solutions also focus on identifying fraudulent websites by creating toolbars that alert the

customer when arriving at a site that is likely to be fraudulent, as eBay uses a toolbar called Spoof stick, but this toolbar cannot prevent damage, even though it indicates that the site is fraudulent. Therefore, the researchers recommend using more than one technical solution to prevent damage.

2) Legal solution

Several laws have been put in place to improve the punishment of identity thieves, and a two-year prison sentence and other legislation will be enforced to deter fraudsters from committing such cyber crimes

3) Business practice

Companies cannot prevent phishing e-mails from reaching their customers, but they can create business practices that help clients learn about phishing e-mails. Here are some suggested practices:

- Addressing clients by name. In general, fraudsters cannot access any personal information.
- Companies require their customers to open a browser window and manually enter URLs instead of requesting personal information in an e-mail message
- Companies must notify their customers of security and privacy policies
- And other mechanisms such as authentication by sending a different password to the customer on their cell phone for each commercial transaction.

4) Education Consumer

Previous solutions are not enough, not preventing phishing e-mails to be received in the inbox. Consumers should be educated on how to protect themselves. The scientific paper reviewed some suggested guidelines:

- Avoid clicking on any link in the e-mails
- Consumers must manually type the URL to confirm the actual website
- Not to send personal information in e-mails
- Read corporate security policies

Finally, it clarified the method for filing a complaint of fraud and identity theft.

In conclusion, the researchers pointed out the need to significantly reduce phishing. No single solution in this paper will end phishing.

Technology providers, the legal system, businesses, and consumers have to work together to protect Internet users and restore confidence in electronic commerce.

From these two studies we propose that the significant solution for phishing attack is to increase the awareness level of society, in addition, the results of the survey that conducted in our research show that the question here is not only to give the solution but also to know how to increase the awareness level, what are best practices for avoiding being a victim of Internet fraud, and How, to whom the user will report when online identity theft or fraud occur?

III. RESEARCH METHODOLOGY

The methodology used in this research is quantitative. The study sample was 271 participants. The survey was applied to measure workers' awareness level in the business sector and understand what the most familiar kind of phishing is and how they usually act to avoid being a victim.

As the result in (Figure1) the sample age groups as 63.5% female and 36.5% male.

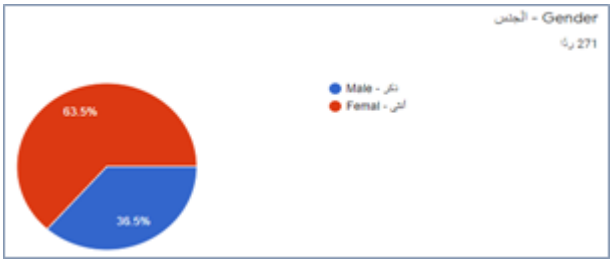

Figure 1: Gender Type

According to the survey results, (Figure2) displays a convergence between the participants' percentages age groups.

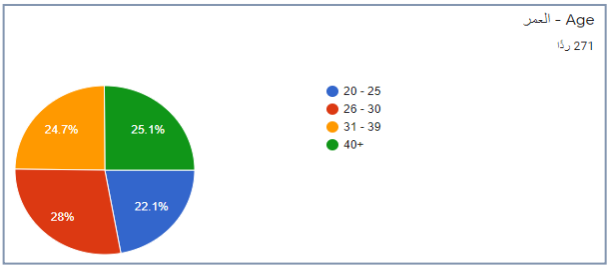

Figure 2: Age groups

The survey was applied to measure workers' awareness levels in different sectors (Figure3).

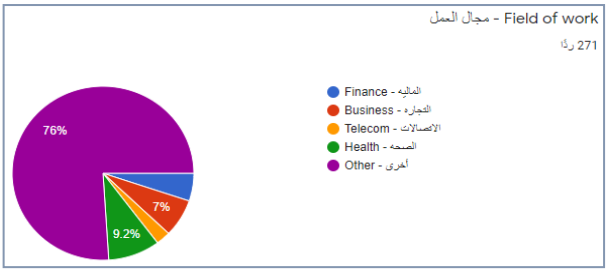

Figure 3: Field of works

(Figure 4) shows that the majority (80.1percent) of participants know the meaning of Cybersecurity (Phishing) terms.

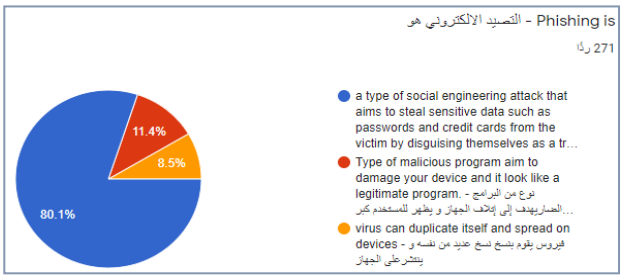

Figure 4: First Question of Questionnaire

The survey results in (Figure 5) show that 19.9 percent of participants are not sure if they had been attacked, while 85.3 percent had not been attacked before, and the remaining are attacked.

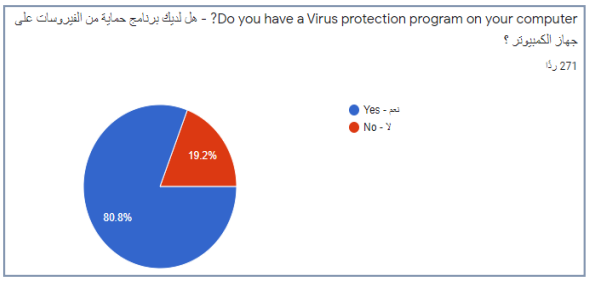

Figure 5: Second Question of Questionnaire

(Figure 6) displays that 51.3% of the participants know about the Firewall feature and its benefits on their computer. In comparison, 34.7% of them did not have an idea about the Firewall, and the remaining are not sure about the Firewall feature.

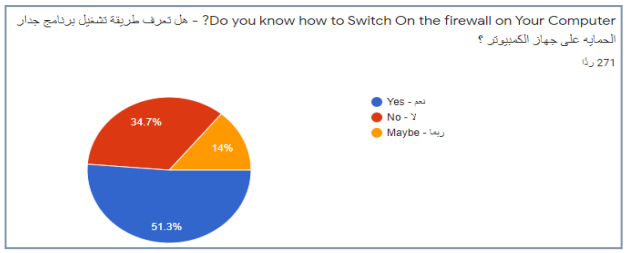

Figure 6: Third Question of Questionnaire

It is necessary to note that from the total number of the participants as shown in (Figure 7) there is 80.8 percent of them have Virus Protection Program on their computer.

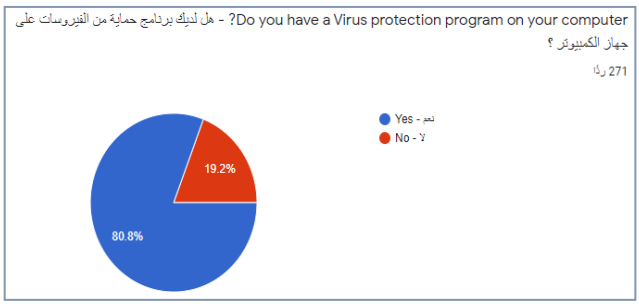

Figure 7: Forth Question of Questionnaire

According to the survey results (Figure 8), 39.9 percent of the participants had been not attacked several times, while 21.8 percent had been attacked one time.

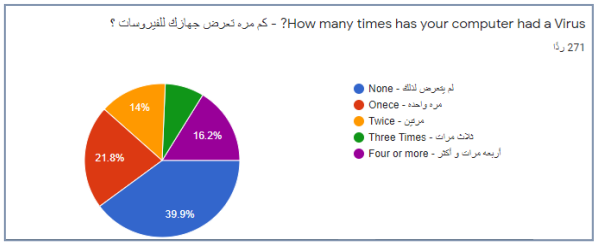

Figure 8: Fifth Question of Questionnaire

(Figure 9) shows that the majority (63.3 percent) of participants trust the technology implemented at their Organization.

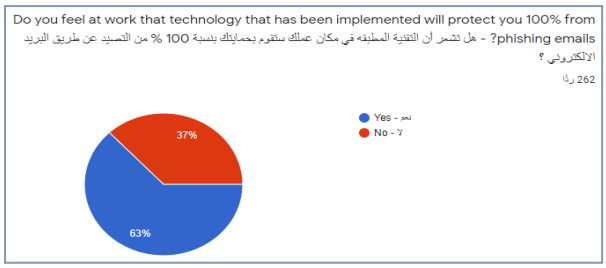

Figure 9: Sixth Question of Questionnaire

Survey results (Figure 10) display a convergence between the participants' percentages, as 35.8% do not know what the phishing e-mail looks like, while 36.2% know about that, and the remaining are not sure about the phishing e-mail styles.

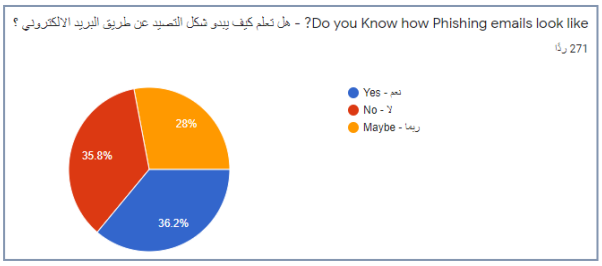

Figure 10: Seventh Question of Questionnaire

According to the survey results (Figure 11), more than an average of participants think that phishing e-mails should have links to other websites.

Figure 11: Eighth Question of Questionnaire

According to the results of the survey, (Figure 12) shows that more than an average of participants checks the source of link before responding.

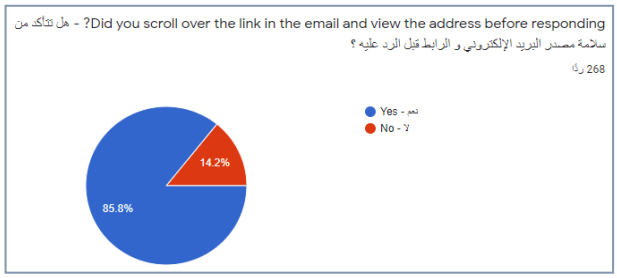

Figure 12: Ninth Question of Questionnaire

The results of the survey, (Figure 13) shows that 65.2 percent of the participants had been look for the e-mail information before responding while 34.8 percent of them had been not checked.

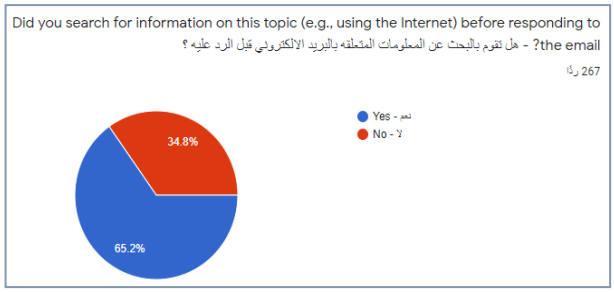

Figure 13: Tenth Question of Questionnaire

(Figure 14) shows that most percent of the participants had a sense about the e-mail's suspicious, while 22.9 percent of them not had this.

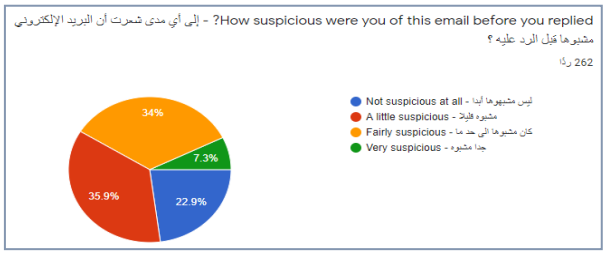

Figure 14: Eleventh Question of Questionnaire

A survey results (Figure 15) display a convergence between the participants' percentages about reading e-mails carefully before responding while 6% of them not very carefully at all.

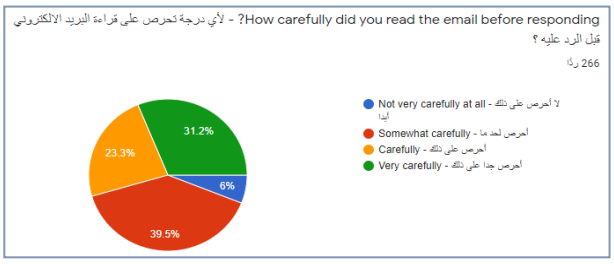

Figure 15: Twelfth Question of Questionnaire

A survey results (Figure 16) shows 39.9 percent out of 271 of participants are not aware about the way to avoid the Phishing, while 27.7percent not sure about that; this means that there is a lack of social awareness because the target category arises not working or familiar with information Technology.

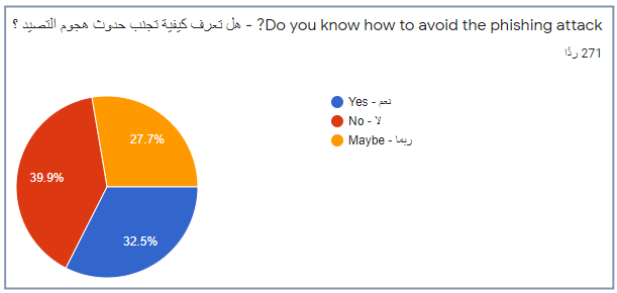

Figure 16: Thirteenth Question of Questionnaire

The result in (Figure 17) shows that 55.7 percent of participants are well-oriented about to whom they should report when facing any kind of Phishing methods, but this not necessarily means they will not be under risk because participants need to be more vigilant to determine the Phishing E-mail, False IP Address, and URL.

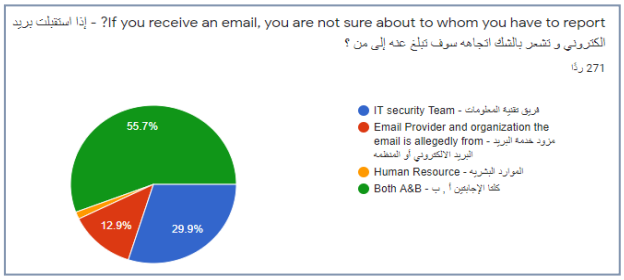

Figure 17: Fourteenth Question of Questionnaire

(Figure 18) indicates that target category are familiar with all the types of the Phishing attack, but as mentioned before, the survey presents a gap of awareness between how the Phishing attack looks like and how to deal with or avoid it.

Figure 18: Last Question of Questionnaire

In conclusion, the survey results show that most participants can recognize phishing e-mails but not aware of how to avoid being a victim. In addition, it shows that most participants trust on the Organizations technology that has been implemented will protect them so, the IT department role of any organization to train the staff and increase the awareness level of how to prevent phishing, to whom they should report, and how they should act when they receive phishing e-mails and increase the sense of responsibility in following Organization's policy.

IV. PHISHING PRETENDING AND PREVENTING

Phishing e-mail messages takes several forms. They might appear to come from the user bank or financial institution, a company the user regularly does business with, such as Microsoft or the use social networking site.

Phishing works by pretending and persuading users to provide personal information by responding to e-mails/SMS or entering confidential data on the website[7].As fears grow over the Corona Virus (COVID-19), pirates are racing to leverage these concerns by exploiting cyber- phishing attacks designed to steal your personal data and money.

Many e-mails pretend to provide new information about the virusor maybe asked to donate money to a charity that is developing a vaccine, taking advantage of your concerns so that you can react without thinking. Or, in exchange for the telling you details of coronavirus outbreaks in your city, you are asked to provide personal information, while some messages go further, asking you to open attachments to find out about safety measures for the virus [8].

Some of the example of the e-mail/SMS subject:

- Verify the user account
- The user e-mail account has been suspended
- Update the user Bank Account
- The user won a lottery.

Cybercriminals are not famous for grammar and spell checking. Professional Businesses and organizations have an editorial team to ensure the consumers get reliable content of high quality. The user must check the validity of the sites that have been visited and read the link well before pressing it, as an additional step can check the links by placing the mouse to see if the title matches the link that was written in the message instead of click the link.

If the user receives an e-mail from any institutions such as Bank, the insurance company or any institution that has business relationship with, asking for any kind of information about sensitive information, contact that Organization to make sure there are no problems with your account with a new e-mail, rather than just hitting reply.

Never post personal data to social media, such as birthdays, vacation plans, addresses or phone numbers [9].

V. PHISHING AWARENESS

Phishing e-mails contain different types, but in general, it always looks legitimate and asks for something confidential. Following are some hints to identify typical phishing e-mails:In any business sector, the IT Department is responsible for filters such as e-mails from reaching the employees by looking for predefined parameters. Exchange Online Protection(EOP), for example, is a specialist for ensuring the protection of Office 365 subscriptions, thereby helping to secure the information through advanced capabilities where filters are focused on combating malware and spam, and thus avoiding any data loss. With a financially backed service level agreement and 99.9 % guaranteed uptime, you can count on e-mailing being always up-to-date. Advanced Threat Protection (ATP) program extends to Word, Excel, PowerPoint, SharePoint Online, and OneDrive for Business. Other improvements also include dynamic delivery, enabling users to instantly receive e-mail messages with attachments scanned for virus detection[10].

Nevertheless, IT cannot block all e-mails by technology, so end-user need to be aware of how to identify and report phishing e-mails and the danger of clicking links in those e-mails. The user should remember that whenever the user receives an e-mail that appears to be from the Organization, IT would never ask the user about ID, Password, or click on a link in a password related e-mail.

A. Role of IT department:

- "Sandboxing" Simple technology is one of the protection mechanisms that isolate programs to stop their disruptive

effects so that these programs do not perform more operations on the rest of the device, which provides more security [13].

- Install monitoring and control tools for each third-party vendor. The tools should allow for an extensive follow-up of any changes and registrations to enter the enterprise's systems.
- Identification of important and sensitive data to be protected. Each Organization has its sensitive data, whether it is financial information, customer lists, or other intellectual property rights. The Organization's management should clarify the type of data that needs to be protected.
- Train and educate staff about internal threats. Most employers educate and train employees on malware, viruses, and cyber-attacks. However, employees must know that they can harm the data by exchanging unnecessary information about the Organization with other employees within the Organization itself.
- Positive reward. Rewarding the department with the most successful tests, through a small bonus or gift cards, will motivate all employees to be more careful[12].

Phishers can damage the Organization's reputation, identity, and financial theft by replying or clicking links inside e-mails.

B. Some tips or advice to help avoid phishing and protect the user

- Most official websites and banks do not ask the user to click on any links within the e-mails they send and do not ask to send the username or password.
- Do not respond to any e-mails requesting personal data or private information. If the user receives a strange e-mail asking him/her to send any personal or private information, delete it immediately. No stranger can ask for any information that belongs to the user.
- Do not click on any links to websites attached to e-mails from people the user does not know. If the user receives a message informing him/her that account has been closed, and the user must click on the link attached to the message to enter his/her username and password to fix the matter, never click on the link. But the user should visit the original site and if there is any problem, make sure that the site will inform the user immediately.
- Do not open any files attached to e-mail messages from people you do not know. If the user receives any message with attached files sent from a stranger or company that the user has not heard about or dealt with before, do not open those attachments because they may simply contain malicious programs that may install themselves on the user's computer.
- Make sure your antivirus software is up to date. If the user clicks on any link in a message or opens an attached file, antivirus software can help protect the user device where the program can detect malicious programs if the user keeps it up to date.
- However, if the user's device is infected, the user should seek help from a specialist to get rid of the malware[14] [15] [16].

C. To protect organization reputation from these kinds of suspicious e-mail, the user has to:

- Report suspicious e-mails by clicking the icon in the top menu of the e-mail message and delete them.
- The user should not provide personal information.
- The user should not respond to suspicious e-mails.
- The user should not click on unknown links or download applications from suspicious websites.
- The user should not open attachments that the user was not expecting.
- The user should not use the company e-mail address for personal things.
- The user should not think it would not happen to him[16] [17].

D. There are some ways to report phishing messages:

If you think you received a fraudulent e-mail, you can report the problem and attach that suspicious message. Reporting suspicious messages to the authorities helps combat identity theft. The following are the steps of how to apply the report[18].

1) forward an e-mail as an attachment in outlook 2016, outlook 2013, or outlook 2010:

First, select the message you want to report, but do not open it. Second, on the Home tab, in the Response group, click More. Third, select forwarding as an attachment. Fourth, on the (To) cell, type the e-mail address of the company or organization, you want to report to the suspicious message. Lastly, click Submit.

2) forward an e-mail message as an attachment in windows mail

Firstly, select the message you want to report, but do not open it. Secondly, on the Actions menu, click Forward as Attachment. Thirdly, on the (To) cell, type the e-mail address of the company or organization you want to report to the suspicious message. Lastly, click Submit.

VI. RECOMMENDATION

In this paper and based on the Data Analysis from the survey; we found that the participants do not have a clear idea about the phishing, how to avoid it and what to do when facing these types of phishing methods. In our opinion, the Cybersecurity authority must increase the awareness level through SMS messages and social media to promote awareness of what exactly phishing is, moving on to the various methods of attacks and how to reduce your risk.

One of the strategies to combat phishing is to train people to recognize and respond to phishing attempts. Training and education are two ways to combat phishing. People should be trained. Below (Figure 19),we show some animation Designed by US Federal Trade Commission to educate citizens about Phishing Method[19].

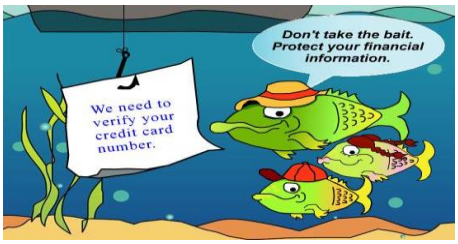

Figure 19: Animation Designed by US Federal Trade Commission

Besides, Saudi Banks launches annually two awareness campaigns, the first aimed at educating the community members about financial fraud and ways to prevent them under the name of "no spread" and the second aims educate the owners of small and medium enterprises in the program to ensure financing of small and medium enterprises [20]. In addition, the awareness could be through Screenshot of Firefox 2.0.0.1 Phishing Suspicious website warning as shown in (Figure20)[21].

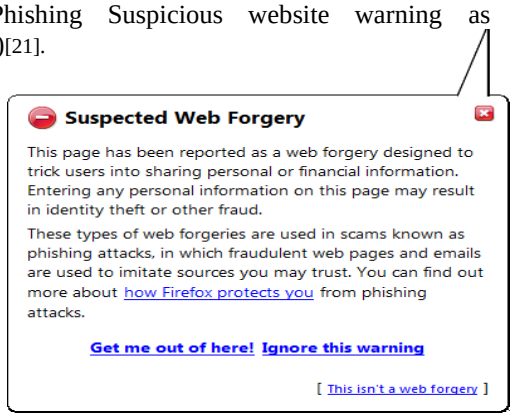

Figure 20: Screenshot of Firefox 2.0.0.1

It is essential for the organization that people who work with it be able to recognize a phishing e- mail. The test is likely to inform the employee of the skills in identifying and dealing with such an accident. However, you should bear in mind that this test does not assess the general capabilities of an employee. Below the details that show phishing indicators that Saudi Aramco Company Phishing Test for their employees: How phishing e-mail messages look like as in (Figure21) and False IP Address (Figure 22-23).

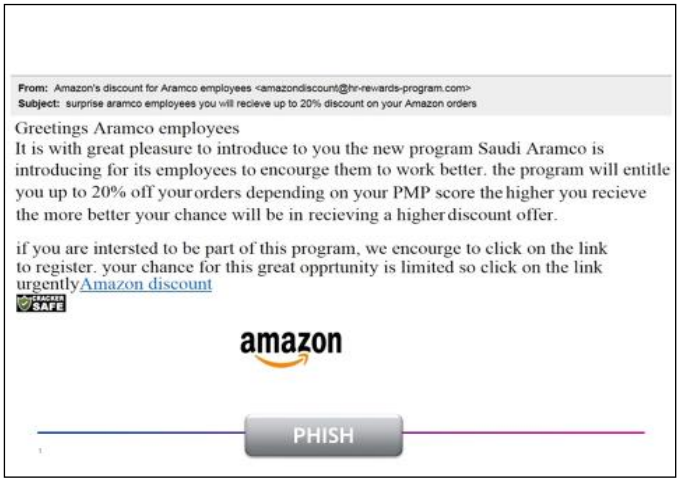

Figure 21: Amazon Phishing Email Messages to Aramco's company Employees

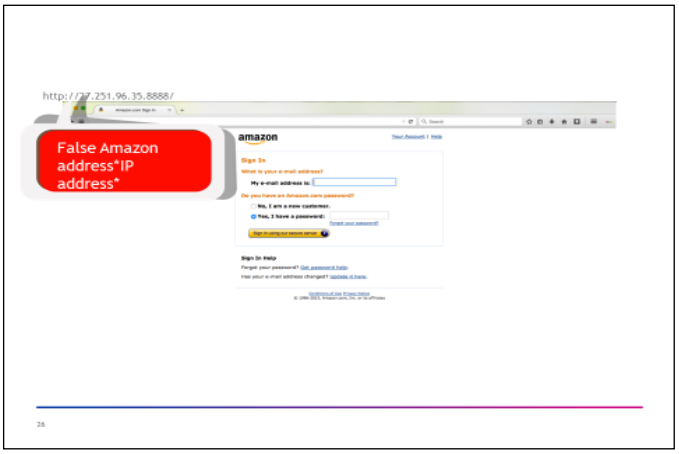

Figure 22: Amazon Phishing Email Messages

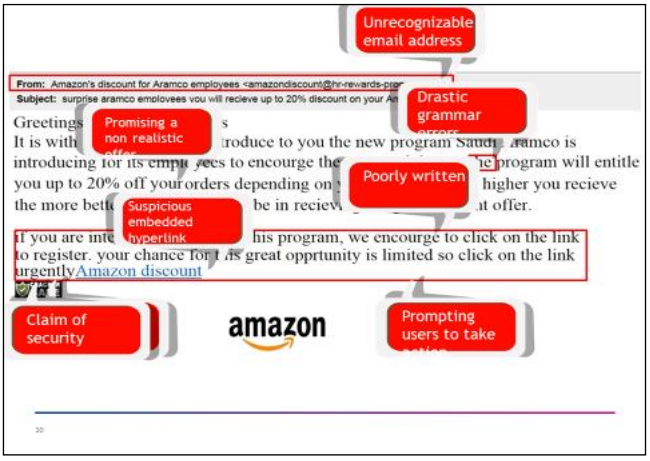

Figure 23: False Amazon IP Address

A. Some practice used by companies to avoid the phishing

- Awareness workshop and presentation
- Policy & Procedures

B. Example of the practice

1) Phishing Failure Policy

In the following (Table I) shows, Consequence for Phishing Failures the company used to take the necessary action against failed employee in the testing of phishing e-mail.

Table II: Consequence for Phishing Failures the company

	1 Failure	2 Failures	3 Failures	4 Failures
Cyber Security Competency Rank	No Impact	No Impact	M	D
E- learning	Yes	Yes	Yes	Yes
Failure Notification	-End user -ISA -Group Leader -Division Head	-End user -ISA -Group Leader -Division Head -Department Head		
Counselling Session(by direct supervisor)	Yes (Verbal)	Yes(Documented)	Yes(Documented)	Yes(Documented)
Account Suspension	No	1 week	2 weeks	Period linked to Corporate Security Investigation (Disciplinary action as per investigation result)

The Cyber Security Competency Rank shows that the employee's annual evaluation is affected according to his/ her performance in the phishing test. What is clear in the table is that the first two times the evaluation is not affected, but after three failures the evaluation is affected as(M) he/ she takes the lowest percentage and thus the annual bonus is a lower percentage, but after the fourth time the employee does not deserve any annual bonus (D). Concerning E-learning, it is an awareness session for the employee about phishing, in which forms and types of phishing are explained, and how to detect fraudulent e-mail messages. As it is shown in failure notification, Identify the people who receive notifications according to the type of failure, whether it is the first, second or third. In addition to that, the table shows how the counselling sessions work, whether verbal or documented. Finally, the employee's account suspended for a certain period, according to the type of failure; the employee cannot receive any e-mail and cannot view any of the personal data. However, if it is the fourth failure, the employee will be transferred to the investigation.

2) Accellion software program

Using software programs to help the organization to communicate with secure content internally and externally and prevent breaches and compliance violations.

Accellion is a platform that allows the organization to exchange the content with third parties, meet the employee's needs with high security of sensitive data from breaching, and block malicious attacks[22].

3) Features of Accellion platform:

- *Visibility:* allow the third parties to communicate visibility and shared sensitive information beyond their enterprise borders. With Accellion's help, businesses have a full vision into how information is shared, by whom it can be accessed, and where it will be stored.
- *Security:*Protect your sensitive information transit against leaks and threats from third-party communications by offers a secure file transfer channel.
- *Simplicity:* all the employees inside the organizations and businesses know how to share sensitive information with the outside world safely and securely without risk by click on the secure sharing button inside the e-mails, web, and mobile, office, and enterprise apps.
- *Flexibility*: Ability of Accellion platform to provide the user with access and share of confidential content in a firm way everywhere and to share the local files easily by Cloud Storage.

However, one of the most limitations is that Fees License should be renewed annually for the software, and this will be costly for the small Organization and business sector [23].

To summarize the research recommendation, firstly, the initial evaluation is considered the first step in raising awareness about phishing. It is an assessment of the current state of the work environment and knowing how ready it is for a possible attack by phishing. The evaluation is via a phishing campaign or other tools.

Secondly, Awareness and Training: the preliminary assessment gives a good idea of the level of awareness to counter phishing attacks within the work environment. It also identifies issues that call for awareness and training.

Thirdly, Campaign Launch: build phishing campaigns and simulations based on the results of the initial evaluation in addition to two main factors: enterprise culture and current malware trends.

Lastly, Smart Reports: a comprehensive report that contains all the details of the process and its results, along with recommendations that help identify weaknesses in the target environment and improve them continuously.

VII. CONCLUSION

The phishing e-mail is the smaller aspect of the overall phishing economy and world's number one cyber-attack method.

This study shows that the reduction of spread phishing is to improve the security technology, good organizational, practices, and awareness training proper application of current technology. Phishing awareness campaigns provide better results when implemented as part of a comprehensive security awareness program.

Experience has taught us that regardless of the amount of investment in IT security solutions, the number of breaches from phishing and sophisticated social engineering attacks continues to grow.

VIII. FUTURE WORK

Further research study and analysis to explore this topic is recommended. However, there are limited studies that have presented on the phishing e-mails problems, how to avoid being a victim and what is the tools and techniques that can be used by the business sector to minimize the frauds in KSA. This research paper can be used to develop new thinking of learning and awareness techniques to prevent phishing e-mails.

IX. ACKNOWLEDGMENT

First, we would like to thank God most of all, because without God we would not be able to do any of this. That has granted us health and knowledge to complete this research.

We would like to express our gratitude and appreciation to Taibah University, Information System department to give us the chance of conducting the research paper.

A very special thanks to our primary supervisor Dr. Abdulrahman Karrar, who guided us throughout this project, his valuable advice contributed substantially to the completion of this research paper. Finally, we are eternally grateful to our friends and family who supported us and offered deep insight into the study.

REFERENCES

[1] Phishing. (2020, April 3). Retrieved fromhttps://en.wikipedia.org/wiki/Phishing

[2] What Is Phishing? Phishing Attack Examples and Definition. (2020, March 30). Retrieved from https://www.cisco.com/c/en/us/products/security/email-security/what-is-phishing.html

[3] Ragan, S. (2018, August 7). What are phishing kits? Web components of phishing attacks explained. Retrieved from https://www.csoonline.com/article/3290417/csos-guide-to-phishing-and-phishing-kits.html

[4] Cyber 101: Deloitte SEA: Risk Advisory. (2019, December 17). Retrieved from https://www2.deloitte.com/my/en/pages/risk/articles/cyber-101.html

[5] Li, Y., Xiong, K., & Li, X. (2019). An Analysis of User Behaviors in Phishing eMail using Machine Learning Techniques. Proceedings of the 16th International Joint Conference on e-Business and Telecommunications. doi: 10.5220/0008119805290534

[6] Analysis of the Phishing Email Problem and Discussion of Possible Solutions. (2005). Proceedings of the 3rd International Workshop on Security in Information Systems. doi: 10.5220/0002564803090318

[7] What is phishing: Attack techniques & scam examples: Imperva. (n.d.). Retrieved from https://www.imperva.com/learn/application-security/phishing-attack-scam/

[8] Jordan, A., & Olson, R. (n.d.). COVID-19: How to avoid cyberattacks when working from home. Retrieved from https://www.weforum.org/agenda/2020/03/covid-19-cyberattacks-working-from-home/

[9] Fruhlinger, J. (2020, February 13). What is phishing? How this cyber-attack works and how to prevent it. Retrieved from https://www.csoonline.com/article/2117843/what-is-phishing-how-this-cyber-attack-works-and-how-to-prevent-it.html

[10] Chrisda. (2021, January 22). Exchange Online Protection (EOP) overview - Office 365. Retrieved February 01, 2021, from https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/exchange-online-protection-overview?view=o365-worldwide
[11] MSFTTracyP. (n.d.). Find and investigate malicious e-mail that was delivered in Office 365, remediate, remedy, remediation, threat protection, threat explorer, protection - Office 365. Retrieved from https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/investigate-malicious-email-that-was-delivered?view=o365-worldwide
[12] News, T. C. (2019, February 8). What is phishing? How this cyber attack works and how to prevent it. Retrieved from https://www.topcybernews.com/what-is-phishing-how-this-cyber-attack-works-and-how-to-prevent-it/
[13] What is Sandbox Security? (2020, March 25). Retrieved from https://www.forcepoint.com/cyber-edu/sandbox-security
[14] "How to Recognize and Avoid Phishing Scams," Consumer Information, 24-Mar-2020. [Online]. Available: https://www.consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams. [Accessed: 03-Apr-2020].
[15] Irwin, L. (2020, January 27). 5 ways to detect a phishing e-mail – with examples. Retrieved from https://www.itgovernance.co.uk/blog/5-ways-to-detect-a-phishing-email
[16] Palmer, D. (2017, September 6). What is phishing? Everything you need to know to protect yourself from scam e-mails and more. Retrieved from https://www.zdnet.com/article/what-is-phishing-how-to-protect-yourself-from-scam-emails-and-more/
[17] InfoTech Solutions. (n.d.). What You Need to Know About Social Engineering & Phishing. Retrieved from https://www.infotech.co.uk/social-engineering-and-phishing-definitive-guide
[18] Phishing Awareness: 8 Things Your Employees Should Understand. (2020, March 12). Retrieved from https://www.vadesecure.com/en/phishing-awareness-training-8-things-employees-understand/
[19] Federal Trade Commission Act of 1914. (2020, March 1). Retrieved from https://en.wikipedia.org/wiki/Federal_Trade_Commission_Act_of_1914
[20] Saudi banks launch campaign to raise awareness of financial fraud and ways of prevention. (2017, November 26). Retrieved from http://saudigazette.com.sa/article/522758
[21] (n.d.). Retrieved from https://www.google.com/search?q=Screenshot+of+Firefox+2.0.0.1+Phishing+Suspicious&rlz=1C1GCEU_enSA849SA849&source=lnms&tbm=isch&sa=X&ved=2ahUKEwi0io-Gx9DoAhWfDWMBHdICDwsQ_AUoAXoECA0QAw&biw=1920&bih=969#imgrc=VQBYGECY36OTIM
[22] Baltimore. (n.d.). Instructions for Accellion. Retrieved from https://www.umaryland.edu/cits/services/accellion/instructions-for-accellion/
[23] Secure File Sharing: Accellion Enterprise Content Firewall. (n.d.). Retrieved fromhttps://www.accellion.com/platform/simple/secure-file-sharing/