Indian Journal of Science and Technology, *Vol 12(25), DOI: 10.17485/ijst/2019/v12i25/145743, July 2019*
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Protecting Users from Phishing Email through Awareness and Training

Ghassan Ahmed Ali*

Department of Information Systems, College of Computer Science and Information Systems, Najran University, Saudi Arabia; gaabdulhabeb@nu.edu.sa, alhabeb@gmail.com

Abstract

Background/Objectives: Most of cyber-attacks start with a phishing emails by deceiving users into acquiring sensitive information. As long human are using the system, there will be a weak part that could be exploited. Many literatures indicates that the main reason of people had been the victim of phishing is a lack of awareness. Several approaches have been used to improve awareness of users; however, the realistic situations in some studies were not applied. Furthermore, environment and organization should be considered when design training methods. **Methods/Statistical Analysis:** The present study was conducted over three years using formative and summative assessments to evaluate students' awareness. This study investigated the most common ways in the classroom of educating students about email phishing email. **Findings:** This study presents the results of email phishing attacks and quizzes conducted to demonstrate how the education can be a powerful tool to increase awareness and protect students from email phishing. This paper also highlights the significance of educational through the classes to increase awareness of email phishing and other security threats. **Improvements/ Applications:** The work could be extended in the future to use more ways of teaching students against phishing attacks.

Keywords: Phishing Email, Formative and Summative Assessments, Cyber Attacks Student Vulnerabilities

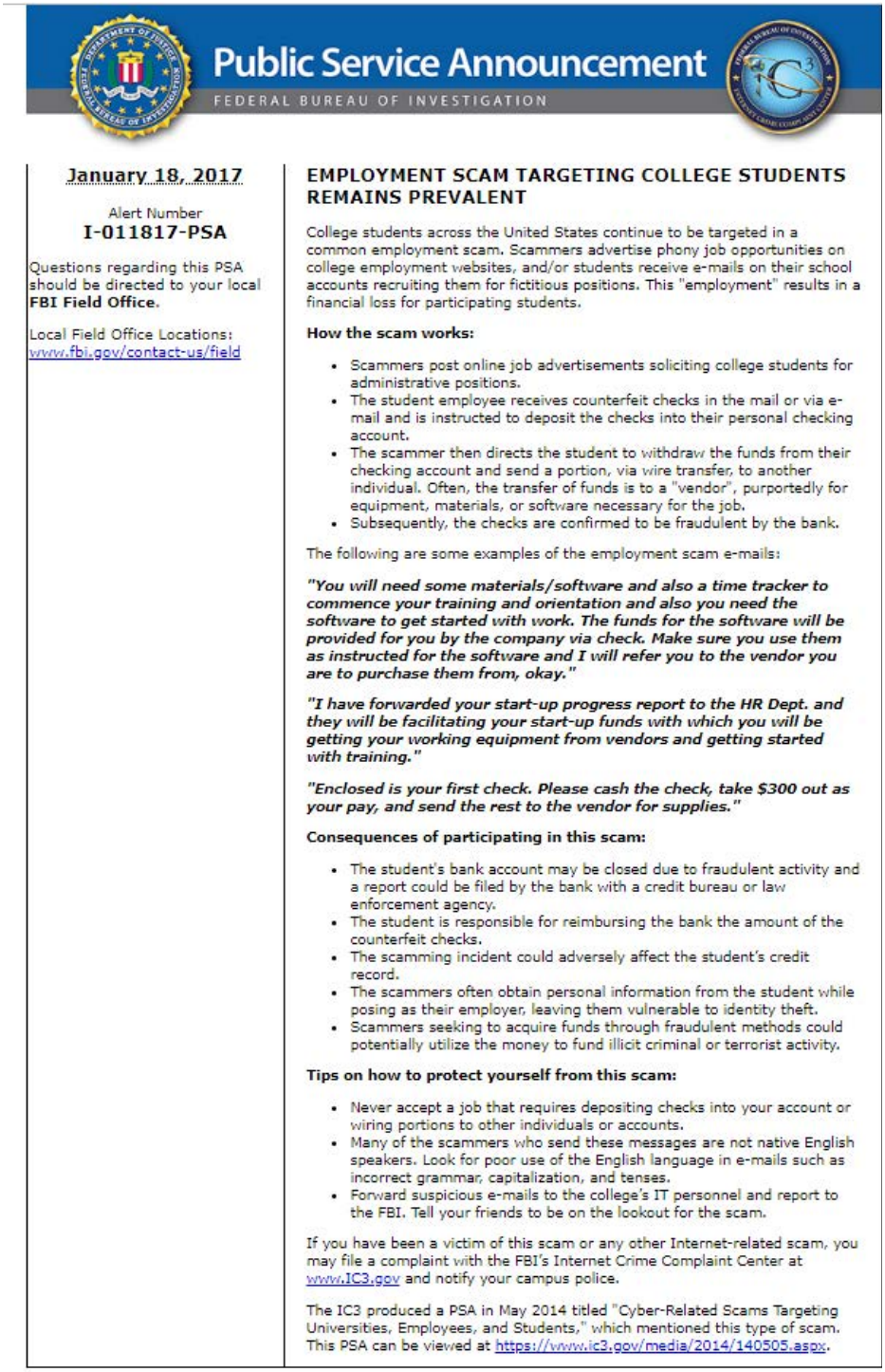
1. Introduction

Email has become a part of daily routines and main method for formal communication for many people and organizations. Specifically, the interest in the education field has been much higher than other sectors[1,2]. Communicating between instructor and students via email is common. For example: call for meeting, collecting data, filling web-survey, submitting marks, or providing guidance for advisees are taking place through email. More specifically, most instructors and faculty staff receive their employment offer letter and job agreement through email. Students also receive emails from advisors, instructors, and administrators to assist them with difficulties or career planning process. Despite the convenience associated for both instructors and students that email still plays main role in their communication, email consider as a primary channel of phishing.

Phishing email is a cybercrime designed to trick someone contacted by email to obtain sensitive information or download files which leads at the end to damage or financial losses to the email recipient. For example, in 2017, the Internet Crime Complaint Center (IC3) received 15,690 complaints related to email account compromise with losses in excess $675 million[3]. The Phishing email targeted specific individuals is one of the riskiest attack[4,5]. Moreover, Phishing email may attract victims by luring them with the promise of a fictitious job or extra money. Figure 1 shows employment scam targeting students. The Figure 1 shows how students could be lured even if the money is deposited to the student bank account phishing life cycle is discussed in section 2. Section 3 reviews previous works on phishing awareness, while Section 3 discusses materials and methods. Results and discussion are presented in Section 4. Section 5 concludes the paper.

2. Phishing Life Cycle

Phishing life cycle starts from attacker by sending a mass emails trying to convince recipient to interact with email included a link as shown in Figure 2. There are two scenarios when a user received a suspicious link: 1- clicking on the link. 2. Interaction activity after clicking on the



Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

January 18, 2017

Alert Number
I-011817-PSA

Questions regarding this PSA should be directed to your local **FBI Field Office.**

Local Field Office Locations: www.fbi.gov/contact-us/field

EMPLOYMENT SCAM TARGETING COLLEGE STUDENTS REMAINS PREVALENT

College students across the United States continue to be targeted in a common employment scam. Scammers advertise phony job opportunities on college employment websites, and/or students receive e-mails on their school accounts recruiting them for fictitious positions. This "employment" results in a financial loss for participating students.

How the scam works:

- Scammers post online job advertisements soliciting college students for administrative positions.
- The student employee receives counterfeit checks in the mail or via e-mail and is instructed to deposit the checks into their personal checking account.
- The scammer then directs the student to withdraw the funds from their checking account and send a portion, via wire transfer, to another individual. Often, the transfer of funds is to a "vendor", purportedly for equipment, materials, or software necessary for the job.
- Subsequently, the checks are confirmed to be fraudulent by the bank.

The following are some examples of the employment scam e-mails:

"You will need some materials/software and also a time tracker to commence your training and orientation and also you need the software to get started with work. The funds for the software will be provided for you by the company via check. Make sure you use them as instructed for the software and I will refer you to the vendor you are to purchase them from, okay."

"I have forwarded your start-up progress report to the HR Dept. and they will be facilitating your start-up funds with which you will be getting your working equipment from vendors and getting started with training."

"Enclosed is your first check. Please cash the check, take $300 out as your pay, and send the rest to the vendor for supplies."

Consequences of participating in this scam:

- The student's bank account may be closed due to fraudulent activity and a report could be filed by the bank with a credit bureau or law enforcement agency.
- The student is responsible for reimbursing the bank the amount of the counterfeit checks.
- The scamming incident could adversely affect the student's credit record.
- The scammers often obtain personal information from the student while posing as their employer, leaving them vulnerable to identity theft.
- Scammers seeking to acquire funds through fraudulent methods could potentially utilize the money to fund illicit criminal or terrorist activity.

Tips on how to protect yourself from this scam:

- Never accept a job that requires depositing checks into your account or wiring portions to other individuals or accounts.
- Many of the scammers who send these messages are not native English speakers. Look for poor use of the English language in e-mails such as incorrect grammar, capitalization, and tenses.
- Forward suspicious e-mails to the college's IT personnel and report to the FBI. Tell your friends to be on the lookout for the scam.

If you have been a victim of this scam or any other Internet-related scam, you may file a complaint with the FBI's Internet Crime Complaint Center at www.IC3.gov and notify your campus police.

The IC3 produced a PSA in May 2014 titled "Cyber-Related Scams Targeting Universities, Employees, and Students," which mentioned this type of scam. This PSA can be viewed at https://www.ic3.gov/media/2014/140505.aspx.

Figure 1. Employment scam targeting students.
Source: IC3. (2017)

suspicious link. The first scenario enables attacker (who sent the suspicious link) to know that the victim has click on the link. As a result of that, attacker knows much information about the victim such as type of device, location, type of victim browser. Moreover, device can be exploit if found vulnerabilities in the target system. It is also a chance for attacker to request the victim to agree to install suspicious software which may be used as a malware later. The second scenario is more dangerous than the first one. Here, the attacker can deceive the victim and show spoof-

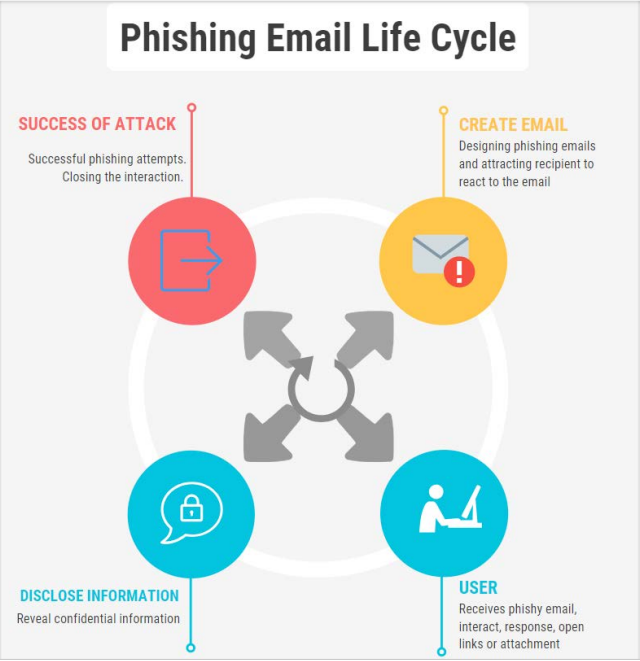


Figure 2. Phishing email life cycle.

ing websites in order to steal victim account. In addition, the details information about victim can be gathered for future used either by spam messages or to exploit victim email next time. Furthermore, attacker can also gain money by let victim to click many times on advertising icons and increase number of fraudulent clicks.

On the one hand, attackers spend times crafting phishing emails and attracting recipient to react to the email. On the other hand, security administrators identifying threats, trying to fill vulnerable holes in the system, testing, and maintaining, but as long human are using the system, there will be a weak part that could be exploited. Many cases specify the vulnerable points of users such as: clicking on suspicious link, sharing personal information via social media, and downloading attachments sent by untrusted source. The key to striking a balance between bad and good or black and white emails and reducing success of Phishing email is based on the awareness of the recipient.

2.1 Phishing Awareness

Several researchers have investigated how to protect users from Phishing Email attacks such as: alarming users from phishing, detecting suspicious attempts, filtering techniques, and checking embedded hyperlink. However, more and more users still become victimized to phishing emails[6]. Several studies point to an association between the level of user awareness and phishing email. According to Bakhshi[7], the main reason of people have been victimized of phishing is a lack of awareness. Awareness plays an important role in security countermeasure[8]. Large studies have confirmed that focus on increasing level of user awareness is an essential key to protect users from phishing. Various methods have been suggested to improve awareness of users such as: to investigate reasons that make users fall in phishing emails and aware users based on these reasons[8], phishing exercises and training[9], game-based training[10], educate users using some factors to increase awareness[11], specific training according to individual differences[12], and provide real-life cases that help to assist awareness. Table 1 summary of recent publications that illustrates the works of how awareness can assist to detect phishing attacks.

Table 1. Summary of recent publications works of the impact of awareness to detect phishing attacks

Methodology	Conclusion
Phishing exercises and training	Exercises increase awareness as a result network security improved
Examined factors that evaluate email	Increase awareness by understanding reasons behind the works of phishing email
Explored of two factors (priming, warnings) that help to increase awareness of attacks and privacy.	User education is essential and key defense against cyber-attack.
Qualitative methodology (interview) security experts to empower users against phishing attack.	Role segmentation and training with real-life cases to increase security awareness
Examine the effectiveness of role playing games	Increasing awareness through training
Determine factors that caused phishing for user security awareness	Feedback, training, and security education beside awareness are required to improve protection of phishing
determines relationship between training and individual differences	Training is helpful in reducing phishing and increasing awareness.

According to[8,9,13], phishing training is one of the techniques that increase awareness and improve result better than other practices like anti-phishing instructions. Different approaches used for training users such as: post-click training[14], an embedded training[15,16], and mindfulness methods[17], however the realistic situations in some studies weren't apply. Furthermore, environment and organization should be considered when design training methods. In addition, to evaluate before and after training and detect the reaction outside training is critical. In this paper, we determine the efficiency of instructor-based or classroom training in which instructor teaches students. Classroom training is more effective in the real world[18] than other methods. There are some arguments and criticisms about time-consuming for this approach, however, the time-consuming criticism is avoided in this study because the trainees are students and the course is mandatory for them in their study plan.

3. Materials and Methods

3.1 Course Environment

One of the learning outcomes of the information system program is: An understanding of professional, ethical, legal, ***security*** and social issues and responsibilities. Some courses must mapping to this LO. One of these courses is Computer Security 429CSS-3 course which corresponding with strong relationship with the above LO. This course is taken by the advanced students male and female before graduation. One Important topic of this course is the awareness of phishing email. In this course an Phishing Email exercises are implemented to evaluate students. The experiments were conducted over three years from first semester of 2016 till the summer semester 2018. Total number of registered students of 429CSS-3 course during the three years were 191 students. Table 2 presents the number of students per semester and gender.

3.2 Formative and Summative Assessments

Two types of assessments were used to evaluate students learning: first is the formative assessment to evaluate ongoing improvement during the course. Second is the summative assessment to evaluate student learning at the end of the course. Assessments were taken as following:

1. **Formative assessment:** *During the First week*, phishing email is sent to students + online phishing awareness quiz.
2. **Formative assessment**: *On the Fifth week*, phishing email is sent to students + online phishing awareness quiz.
3. **Summative Assessment**: *On the Last week*, phishing email is sent to students + online phishing awareness quiz.

3.2.1 Phishing Emails

Three simulated emails phishing that contain attractive phishing techniques are planned to be sent to students. These simulated emails are written in Arabic and English languages since the instructions of the college are conducting in English but not all students have a good level of English and they may ignore the emails because of language difficulty. Emails were sent to students' emails according to topic and times as following:

- First email sent on first week requested personal information.
- Second email sent on fifth week requested account verification.
- Third email sent on the last week asked students to download an attachment file.

3.2.2 Phishing Awareness Quizzes

Three automated quizzes (QuizNo1, QuizNo2, and QuizNo3 respectively) are presented to measure students'

Table 2. Number of students per semester and gender

Gender	Semester						
	1_2016	2_2016	1_2017	2-2017	1-2018	2-2018	3-2018
Male	14	13	17	10	15	25	12
Female	25	12	10	15	8	5	10

vulnerability to e-mail phishing. Each quiz contains questions for a group of emails. Emails display one by one to students in order to determine and make decision if the e-mail message is a phishing e-mail or not by answering Yes or No. At the end of the quizzes, students are taken their scores along with the false and correct answers. This kind of awareness evaluation is a well-planned without causing students to be worried. Furthermore, quizzes questions are used as a learning tool.

In the first week, students are required to take Quiz. No1 as evaluation of pre-course. Quiz.No1 is not planned to evaluate knowledge of students, but rather an assessment of what the students know about the phishing. The pre-course assessment could increase skills acquisition and retention as well[19].

During the fifth week, students encountered Quiz. No2 to evaluate their levels comparing to Quiz.No1. Quiz.No2 is planned to be as a fine-tune to have continues improvement of learning. Ten new emails in addition to the previous emails in QuizNo1 are displayed to evaluate the course transfer. Furthermore, Quiz.No2 assesses whether behaviors and skills are improved during previous weeks or not.

In the last week, QuizNo3 is administered at the end of the course to measure the course learning outcomes. In this quiz, thirty emails are displayed to the students to evaluate the level of the students by comparing the results of students with previous quizzes. This quiz is also taken by other students who had not registered to Computer Security 429CSS-3 course to compare later with students who registered the course.

4. Results and Discussion

Results are shown by overall percentage in four aspects as following:

4.1 Results of Phishing Email

Results show that more than half of the students had clicked the link and were interactive with the phishing email on the first week. A small percentage of students 12% ignored the phishing email while about one-third of the students clicked on the link in the email and they didn't continue to the phishing website. It is obvious from the first week results that most students were not knowledgeable about the phishing emails.

In the fifth week, there is a clear difference in the results, as about half of the students ignored the email and the number of students who were interactive with the email or click on the link only were decreased. This result indicates the improvement of the students' knowledge against the phishing emails.

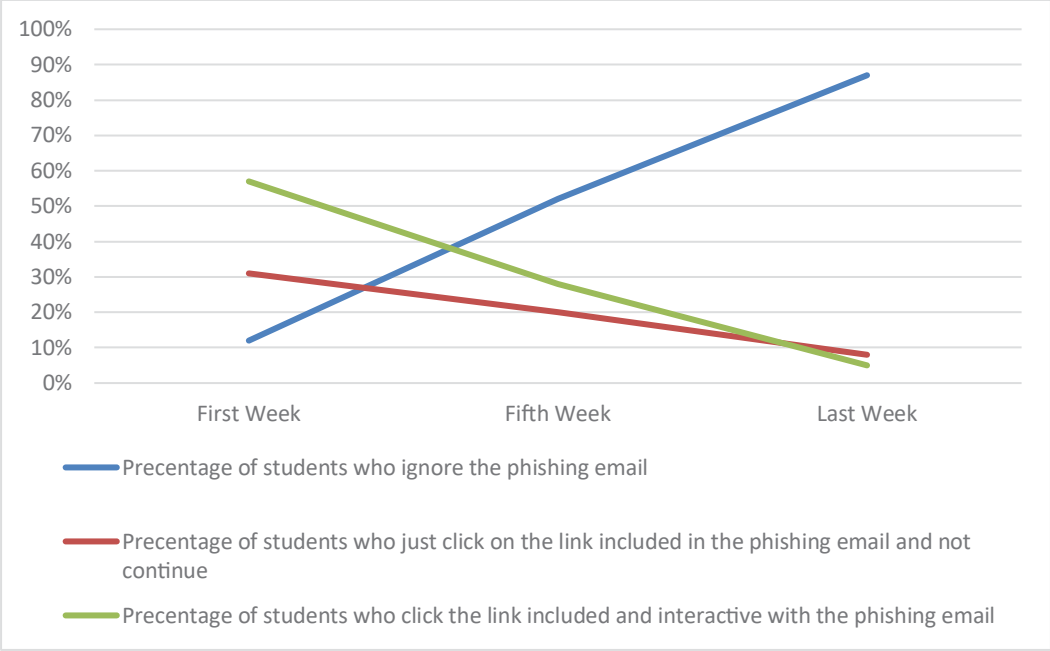


Figure 3. Results of phishing email attempts.

The last week evaluation shows a great reduction of Phishing Email failures, the percentage of students who ignored the phishing email is increasing to 87% and the percentage of students who clicked the link included and were interactive with the phishing email is declining to 5%. Accordingly, the results show the value of the education via classes in decreasing the risk of Phishing Email. Result of phishing email is shown in Figure 3.

4.2 Results of Quizzes

Most students got low score in quiz 1 in the first week as shown in Figure 4. It can be seen from Figure 4 that more than 80% of students cannot distinguish a phishing email from a legitimate. Sixteen percent of the students got average score whereas only 3% of students got high score. The students' scores in the first week reflect that most students were not aware of a phishing emails.

From Figure 4, it can be seen the significance difference of recognizing phishing emails in the fifth week. Forty two percent of students got average score and 43% got low score whereas 15% got high score. The assessment of the fifth week indicates the evaluation of a class improvement of students' level of awareness. The evaluation results generally show the effectiveness of class-based to increase the awareness about Phishing Email to students.

The summative assessments assess students at the end of the course. Table shows the 71% of students got high score of the last week quiz and only 9% of students got low score. This result indicates the correlation with the formative assessments to ensure that used quiz is an effective tool for measurement. Furthermore, it is obvious that majority of students can distinguish between phishing and a legitimate emails after receiving a phishing awareness topic.

4.3 Results of Comparing Registered and Non-registered Students

To ensure the effectiveness of the Computer Security 429CSS-3 course in increasing the awareness of phishing emails; it would be interesting to compare results of students enrolled in Computer Security 429CSS-3 course with the students who are not enrolled in the course. Figure 5 shows graphically the results of the comparison between the results of the last week quiz against the students who are not enrolled in the course. From the Figure 5, it can be seen the big difference in the results of students who enrolled with the students who are not enrolled in the course. Eighty five percent of students who were not enrolled the course got low score whereas only 9% of enrolled students got low score. Likewise, only 2% of students who were not enrolled the course got high score whereas 71% of enrolled students got high score. The result of the last week quiz were used to evaluate student learning at the end of the 429CSS-3 course and had been selected for a comparison.

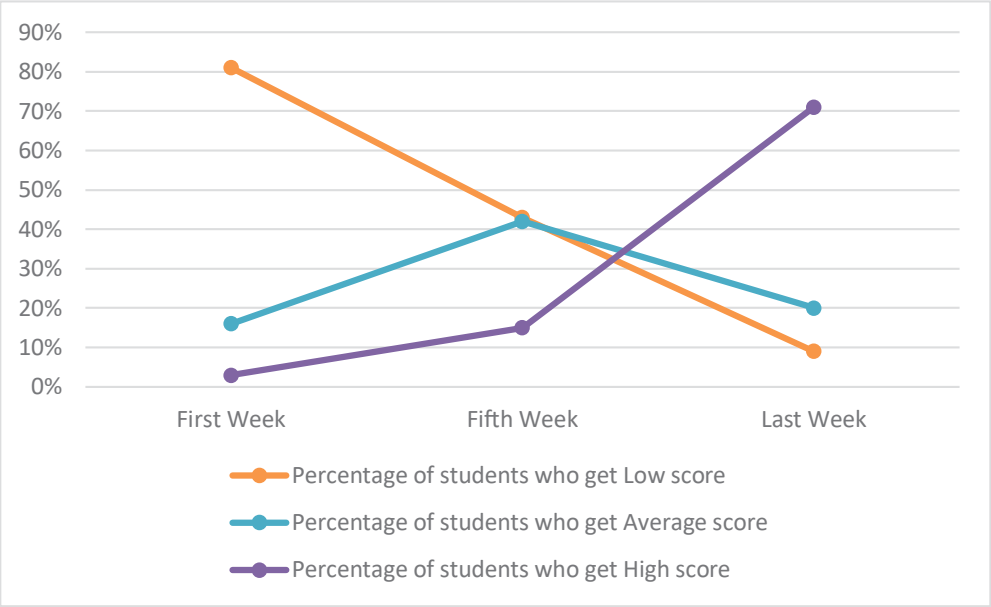


Figure 4. Results of quizzes.

4.4 Results of Assessing Knowledge Retention

Many studies consider the knowledge retention as important value of education[20] which shows the ability of learners to retain what has been learned after a period of time. According to[21,22], learners gained improvement in knowledge and able to remember and identify phishing challenges after training. One of the measurements of knowledge retention commonly used is a true-false question[23]. In our case, Quiz No3 is used to measure the knowledge retention of students after 3 months of the studied course. Emails display one by one to students in order to determine if the e-mail message is a phishing e-mail or not by answering Yes or No. The result shows that the level of retention is high 80% even after three months of the course. Finally, the result is compared with the results of last week of the course to determine the knowledge loss as shown in Figure 6. From the results, we can conclude that the studied course was unforgettable for most students.

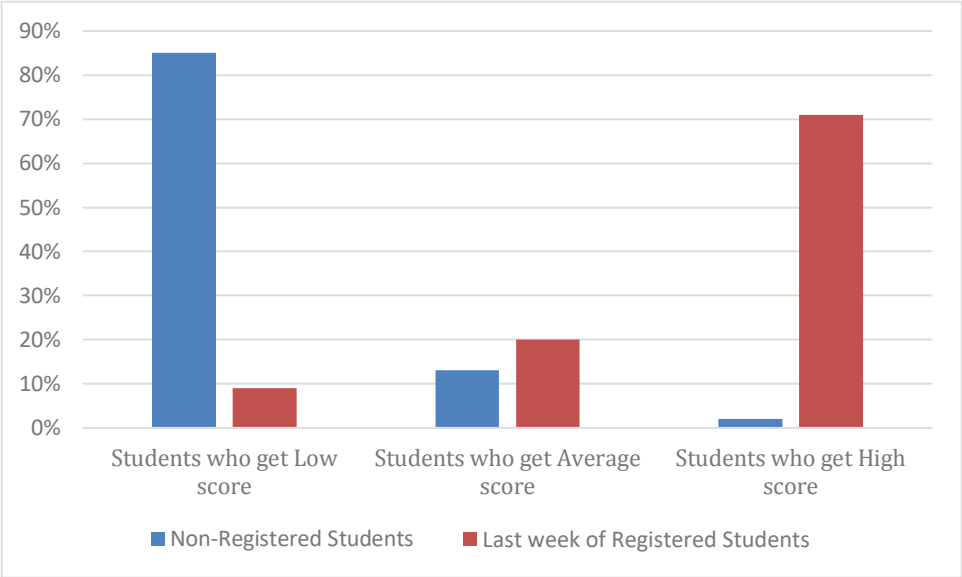


Figure 5. Results of registered vs non-registered students.

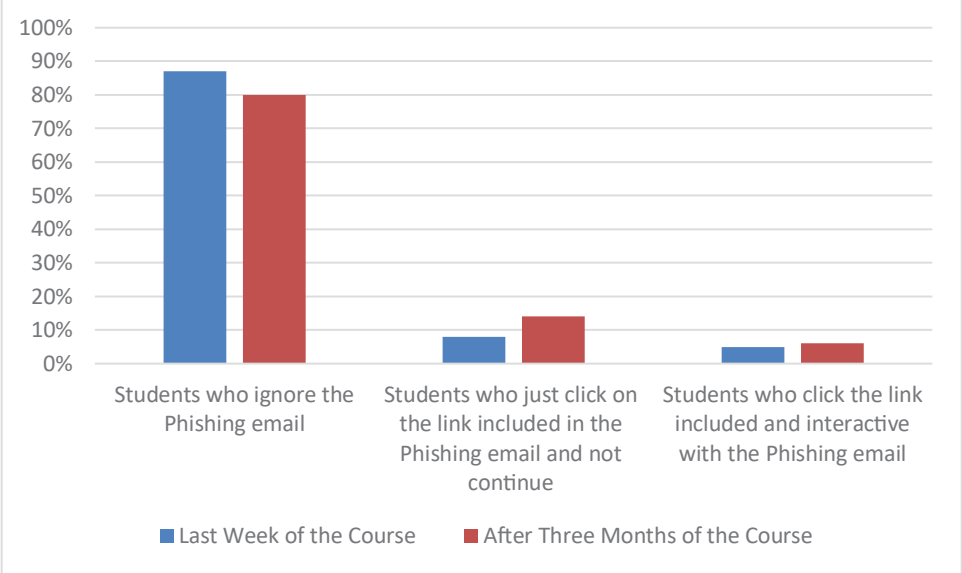


Figure 6. Results of knowledge retention.

5. Conclusion

Most students become victims to phishing emails in order to disclose private information. On the same time, many methods are improving to increase the awareness of Phishing Email. This study investigated the most common ways classroom of educating students about Phishing Email. The results showed the fruitful of classroom training in increasing the students' awareness of Phishing Email. Formative and summative evaluation before, during, and after were taken to ensure the transfer of knowledge and to retain knowledge after three months as well. The work could be extended in the future to use more ways of teaching students against email phishing attacks.

6. References

1. James N. Using email interviews in qualitative educational research: Creating space to think and time to talk. International Journal of Qualitative Studies in Education. 2016; 29(2):150–63. https://doi.org/10.1080/09518398.2015.1017848
2. Gilbert S. AAHESGIT: New thread email. Elect. Comm., personal communication; 1996
3. Internet crime report [Internet]. [cited 2017]. Available from: https://pdf.ic3.gov/2017_IC3Report.pdf.
4. Junger M, Montoya L, Overink FJ. Priming and warnings are not effective to prevent social engineering attacks. Computers in Human Behavior. 2017; 66:75–87. https://doi.org/10.1016/j.chb.2016.09.012
5. Thomas J. Individual cyber security: Empowering employees to resist spear phishing to prevent identity theft and ransom ware attacks [Internet]. [cited 2018]. Available from: http://www.ccsenet.org/journal/index.php/ijbm/article/view/74724. https://doi.org/10.5539/ijbm.v13n6p1
6. Alsharnouby M, Alaca F, Chiasson S. Why phishing still works: User strategies for combating phishing attacks. International Journal of Human-Computer Studies. 2015; 82:69–82. https://doi.org/10.1016/j.ijhcs.2015.05.005
7. Bakhshi T. Social engineering: Revisiting end-user awareness and susceptibility to classic attack vectors. 2017 13th International Conference on Emerging technologies; 2017. https://doi.org/10.1109/ICET.2017.8281653. PMCid:PMC5556433
8. Aldawood H, Skinner G. An academic review of current industrial and commercial cyber security social engineering solutions. Proceedings of the 3rd International Conference on Cryptography, Security and Privacy; 2019. p. 110–15. https://doi.org/10.1145/3309074.3309083
9. Dodge RC, Carver C, Ferguson AJ. Phishing for user security awareness. Computers and Security. 2007; 26(1):73–80. https://doi.org/10.1016/j.cose.2006.10.009
10. Williams EJ, Polage D. How persuasive is phishing email? The role of authentic design, influence and current events in email judgments. Behaviour and Information Technology. 2019; 38(2):184–97 https://doi.org/10.1080/0144929X.2018.1519599
11. Hale ML, Gamble RF, Gamble P. Cyber Phishing: A game-based platform for phishing awareness testing. 2015 48th Hawaii International Conference on System Sciences; 2015. p. 5260–9. https://doi.org/10.1109/HICSS.2015.670
12. Bada M, Sasse A. Cyber security awareness campaigns why do they fail to change behaviour? International Conference on Cyber Security for Sustainable Society; 2014. p. 1–38.
13. Mayhorn CB, Nyeste PG. Training users to counteract phishing. Work. 2012; 41(S1):3549–52.
14. Yar M, Steinmetz KF. Cybercrime and society. SAGE Publications Limited; 2006. p. 185.
15. Kumaraguru P, Rhee Y, Acquisti A, Cranor LF, Hong J, Nunge E. Protecting people from phishing: The design and evaluation of an embedded training email system. Proceedings of the SIGCHI conference on Human factors in computing systems; 2007. p. 905–14. https://doi.org/10.1145/1240624.1240760
16. Caputo DD, Pfleeger SL, Freeman JD, Johnson ME. Going spear phishing: Exploring embedded training and awareness. IEEE Security and Privacy. 2014; 12(1):28–38. https://doi.org/10.1109/MSP.2013.106
17. Jensen ML, Dinger M, Wright RT, Thatcher JB. Training to mitigate phishing attacks using mindfulness techniques. Journal of Management Information Systems. 2017; 34(2):597–626 https://doi.org/10.1080/07421222.2017.1334499
18. Booker KC, Merriweather L, Campbell-Whatley G. The effects of diversity training on faculty and students' classroom experiences. International Journal for the Scholarship of Teaching and Learning. 2016; 10(1):9. https://doi.org/10.20429/ijsotl.2016.100103
19. Li Q, Zhou RH, Liu J, Lin J, Ma EL, Liang P, Xiao H. Pre-training evaluation and feedback improved skills retention of basic life support in medical students. Resuscitation. 2013; 84(9):1274–8 https://doi.org/10.1016/j.resuscitation.2013.04.017. PMid:2366515520.
20. Ausubel DP. The acquisition and retention of knowledge: A cognitive view. Springer Science and Business Media; 2012.
21. Hung IC, Chen NS. Embodied interactive video lectures for improving learning comprehension and retention. Computers and Education. 2018; 117:116–31. https://doi.org/10.1016/j.compedu.2017.10.005

22. Kumaraguru P, Cranshaw J, Acquisti A, Cranor L, Hong J, Blair MA, Pham T. School of phish: A real-world evaluation of anti-phishing training. Proceedings of the 5th Symposium on Usable Privacy and Security; 2009. p. 3. https://doi.org/10.1145/1572532.1572536

23. Arzi HJ, Ben-Zvi R, Ganiel U. Forgetting versus savings: The many facets of long-term retention. Science Education. 1986; 70(2):171–88. https://doi.org/10.1002/sce.3730700211