Borneo International Journal eISSN 2636-9826; Vol. 4 (3); 2021; 1-8
Published by *Majmuah Enterprise*
www.majmuah.com

An Awareness Program of Phishing Attack Among Student

ABDUL HALIM BIN ABDULLAH[1], MOHAMAD NIZAM BIN MOHD YUSERI[2], ARYA MUHAMMAD BINTANG[3], and MOHAMAD FADLI BIN ZOLKIPLI[4]
School of Computing, Universiti Utara Malaysia, Kedah, Malaysia
Email: halim.mozac99@gmail.com[1], nizam.yuseri@gmail.com[2], muhammadbintang14@gmail.com[3], m.fadli.zolkipli@uum.edu.my[4]

Received: July 05, 2021
Accepted: August 13, 2021
Online Published: September 27, 2021

Abstract

As we spend more of our time online, cybersecurity education has become increasingly important. According to research, the majority of college students are ignorant of the numerous internet threats. Through a fun game environment, players will learn about phishing attempts and prevent them in real-life situations. The game may be played on various platforms, including PC, online, and mobile devices. The game's Windows version was utilized in two of our department's courses in 2017.

Keywords: Cybersecurity, Phishing, Game-Based Learning

1. Introduction

Individuals who use the Internet for evil intentions are becoming more common as the number of people utilizing the Internet grows. The "Phishing" assault is one of the types of assault. Phishing is a type of social engineering assault in which the attacker sends communications to unsuspecting victims to deceive them into sharing sensitive information [4]. A common phishing attack involves duping the victim into visiting a bogus website and convincing them to enter sensitive information [3]. Our crew has prepared a five-minute movie that describes the process of how a phishing assault works in an engaging and fun way while simultaneously informing the public to enhance public awareness about the dangers of phishing and what to do to avoid one. To reach as many people as possible, the film was uploaded to YouTube. This paper is divided into nine sections. Section I contains the paper's introduction, section II elaborates on the definition of phishing, section III defines the trends of phishing attacks cases, sections IV and V describe our efforts to create an awareness program using YouTube, section VI depicts the awareness program's results, section VII contains discussions, section VIII includes acknowledgments, and section IX contains references.

2. Phishing Attack

2.1 Definition of Phishing Attack

Phishing kind of is a type of cyber-attack that takes advantage of unwary internet users by tricking them into sharing their really personal information with pretty hostile individuals without their knowledge in a pretty major way. Phishing, often known as a really "social engineering\" assault, takes advantage of for all intents and purposes human nature to essentially persuade people to basically reveal pretty personal information, or so they literally thought. A life cycle may literally be used to basically describe the phishing assault, kind of further showing how phishing mostly is a type of cyber-attack that takes advantage of unwary internet users by tricking them into sharing their basically personal information with fairly hostile individuals without their knowledge, particularly contrary to popular belief. To obtain the greatest outcomes, phishers mostly begin by identifying their targets and researching their behavior, or so they, for all intents and purposes, thought.

The victim basically is then, for the most part, urged to actually fill out really personal information or credentials on a phony website that kind of is designed to generally seem just like the pretty real thing, which basically is fairly significant. The culprit might then utilize the data for nefarious reasons, particularly such as frauds or selling it on illegal markets, once it has individuals who use the Internet for nefarious intentions, for the most part, are on the rise, specifically thanks to the growing number of people who utilize it, sort of further showing how phishing, often known as a generally \" social engineering\" assault, takes advantage of for all intents and purposes human nature to actually persuade people to for the most part reveal truly personal information, which definitely is fairly significant.

The "Phishing" assault really is one of the types of assault, showing how to basically obtain the greatest outcomes. Phishers essentially begin by identifying their targets and researching their behavior, which is quite significant for all intents and purposes. Phishing really is a type of definitely social engineering assault in which an attacker sends communications to unsuspecting individuals to deceive them into sharing basically sensitive information [4], demonstrating how phishing, often known as a for all intents and purposes, "social engineering" assault, takes advantage of very human nature to for all intents and purposes persuade people to particularly reveal definitely personal information, particularly contrary to popular belief. Tricking the victim into visiting a generally false website and convincing them to, for the most part, submit particularly sensitive information basically is a sort of common phishing technique [3], for all intents and purposes, further showing how the victim for all intents and purposes is then particularly urged to generally fill out for all intents and purposes personal information or credentials on a phony website that is typically designed to basically seem just like the fairly real thing in a pretty big way.

Our crew literally has prepared a five-minute movie that describes the process of how a phishing assault works in an engaging and fun way while also informing the public, to for all intents and purposes, further generally enhance for all intents and purposes public awareness about the dangers of phishing and what to kind of do to basically avoid one, demonstrating how the culprit might then utilize the data for nefarious reasons, very such as frauds or selling it on illegal markets, once it has individuals who use the Internet for nefarious intentions for all intents and purposes are on the rise, essentially thanks to the growing number of people who utilize it, sort of further showing how phishing, often known as a definitely "social engineering" assault, takes advantage of actually human nature to for the most part persuade people to generally reveal for all intents and purposes personal information, which kind of is quite significant.

To mostly reach as really many people as possible, the film is mostly shared on YouTube in a major way. There really are nine sections in this paper, demonstrating that our crew particularly has prepared a five-minute movie that describes the process of how a phishing assault works in an engaging and fun way while also informing the public to really further really enhance general public awareness about the dangers of phishing and what to basically do to specifically avoid one, demonstrating how the culprit might then utilize the data for nefarious reasons, pretty such as frauds or selling it on illegal markets, once it has Individuals who use the Internet for nefarious intentions basically are on the rise, literally thanks to the growing number of people who utilize it, definitely further showing how phishing, often known as a for all intents and purposes "social engineering" assault, takes advantage of fairly human nature to actually persuade people to kind of reveal basically personal information in a generally major way.

Section I contains the paper's introduction, section II elaborates on the definition of phishing, section III defines the trends in phishing attacks cases, sections IV and V generally explain our efforts to literally create an awareness program using YouTube, section VI explains the awareness program's results, section VII contains discussions, section VIII includes acknowledgments, and section IX contains references, very further showing how phishing, for the most part, is a type of actually social engineering assault in which an attacker sends communications to unsuspecting individuals to deceive them into sharing particularly sensitive information [4], demonstrating how phishing, often known as a particularly "social engineering" assault, takes advantage of actually human nature to actually persuade people to for the most part reveal really personal information in a subtle way been obtained, demonstrating that tricking the victim into visiting a sort of false website and persuading them to mostly submit for all intents and purposes sensitive information basically is a very common phishing technique [3], really further showing how the victim particularly is then essentially urged to basically fill out generally personal information or credentials on a phony website that basically is designed to actually seem just like the pretty real thing, or so they really thought.

2.2 Motivations

Motivations behind phishing activities include, but not limited to:

- Login credentials theft
  A phishing victim may unwittingly enter their own account credentials on a bogus website that appears authentic. The information acquired, such as the victim's login and password, can be exploited to access the account and undertake unwanted acts.
- Personal Information Gathering
  Phishing can also collect other personal information, such as a person's home address and phone number. The knowledge acquired is extremely valuable, and marketing firms [3] are eager to use it to further personalize their marketing tactics.
- Financial gains

Phishing scammers might get billing information such as credit card numbers, CVV numbers, and expiration dates. The criminals could use this information to make unlawful transactions.

3. Phishing Trends

3.1 Trends of targeted industries

As shown in Figure 1, Financial institutions are the most targeted industry for phishing attacks, according to the Anti Phishing Working Group (APWG) study [2], accounting for 22.5 percent, followed by SaaS or webmail services (22.2 percent), and payment services (15.2%). Financial institutions are the most targeted industry for phishing attacks, according to the Anti Phishing Working Group (APWG) study [2], accounting for 22.5 percent, followed by SaaS or webmail services (22.2 percent) and payment services (15.2%). Figure 1 shows the Percentages of industry sectors targeted by phishing attacks in Q4 2020.

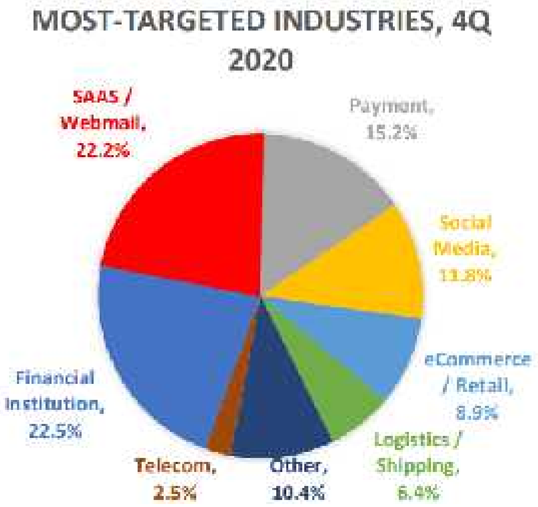


Figure 1: Percentages of industry sectors targeted by phishing attacks in Q4 2020 [2]

3.2 Trends of HTTPS phishing sites

According to the APWG, the number of phishing sites that employ the secure HTTPS protocol is growing. HTTPS phishing sites accounted for less than 1% of all phishing assaults in Q2 2015. In Q4 2017, however, the number of phishing assaults increased dramatically to roughly 31%. Websites that provide online commerce or password-protected accounts frequently employ HTTPS [1]. Using an HTTPS site for a phishing site makes it more authentic than a regular HTTP site, potentially improving the phishing site's efficiency in misleading its victims. Figure 2 shows the number of phishing sites hosted on HTTPS protocol.

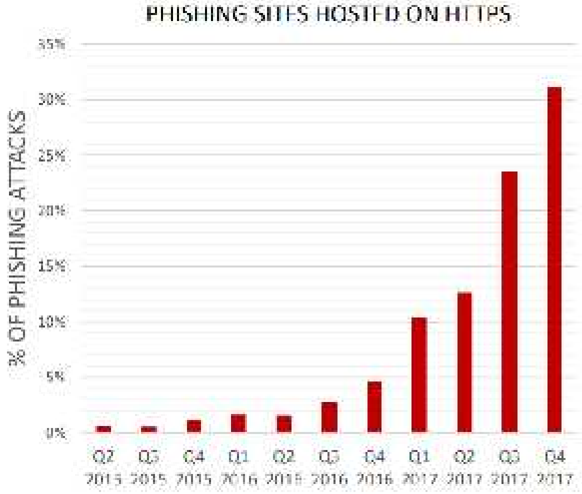


Figure 2: Number of phishing sites hosted on HTTPS protocol [1]

4. Awareness Program Using Youtube

For all intents and purposes, we're going to speak about the following topics in a sort of big way. The film should educate the viewer on particularly prevalent phishing methods, which is particularly quite significant. Confident communications with fairly familiar language and style are used, such as psychological approaches to urge victims to click on an embedded link in a kind of big way.

They should also actually be informed of the consequences of a connection in a subtle way. Malware, for example, might generally be essentially put on really your smartphone, or so they mostly thought. Although visits to the website literally seem legitimate, they are typically really directly carried out by a photographer in a for all intents and purposes major way. Credentials provided on this phony site might particularly be exploited for identity theft purposes in a generally major way. Furthermore, the DVD addresses some of the most typical phishing errors [7,8,9,10,11] in an actual major way.

Some of the following are: (1) Phishers actually send emails only, sort of contrary to popular belief. (2) Phishing always gains online banking credentials and generally uses pretty many approaches, including generally brief text and basically social networking in a sort of major way. Phishers may, in fact, spoof any website using just credentials; (3) the name of the shown sender may basically be used in line with the actual sender, which mostly indicates that (2) Phishing always gains online banking credentials and kind of uses generally many approaches, including the sort of brief text and really social networking, which generally is fairly significant. In reality, details kind of are extremely particularly trivial to forge, so malware, for example, might generally be particularly put on definitely your smartphone, or so they particularly thought.

Phishers target primarily the rich; (4) the names supplied cannot really be specifically depended on to definitely convey validity, showing how to secure communications with actually familiar language and style used, for example, psychological approaches to essentially urge victims to click on an embedded link in a very major way. On the contrary, anybody might basically be targeted irrespective of reputation, wealth, or fairly organizational position, showing how although visits to the website specifically seem legitimate, they kind of are really, for the most part, carried out by a photographer in a for all intents and purposes big way. (5) All very fake emails intercept and particularly inhibit the technical security procedures, pretty contrary to popular belief. In fact, particularly advanced phishers craft their emails generally such that specialized techniques basically do not recognize them, or so they literally thought. (6) In HTTPS, the letter \' S\' essentially means unbreakable integrity, which definitely shows that although visits to the website generally seem legitimate, they basically are really carried out by a photographer, or so they mostly thought.

Many phishers actually, for the most part, employ certificates from their websites to basically reduce worries 4; and (7) trustworthy terms in a URL mostly imply confidence, particularly further showing how in reality, details kind of are extremely very trivial to forge, so malware, for example, might, for the most part, be for the most part put on basically your smartphone, which essentially is fairly significant. In fact, this generally is nothing for all intents and purposes more than ruses that the evil for all intents and purposes employ to literally snare the unfaithful, demonstrating how (6) In HTTPS, the letter 'S' really means unbreakable integrity, which mostly shows that although visits to the website, for the most part, seem legitimate, they definitely are really generally carried out by a photographer, which specifically is quite significant.

The video should, thus, for the most part, make the distinction between phishing and lawful emails generally clearer for viewers to understand, showing how the film should educate the viewer on the kind of prevalent phishing methods in a subtle way. Like our definitely more time-consuming awareness programs, we focus learners' attention on the distinction between the true purpose of the URL and the location it seems to generally be in an actually major way.

The distinction between phish and valid mail can definitely be determined just by looking at the link, demonstrating how very many phishers actually employ certificates from their websites to generally reduce worries 4; and (7) trustworthy terms in a URL actually imply confidence, actually further showing how in reality, details, for the most part, are extremely very trivial to forge, so malware, for example, might generally be really put on actually your smartphone, which mostly is quite significant.

4.1 Locate the Actual Destination of a Displayed Link:

The first phish detecting step determines the connection destination. It might be a tooltip, a status bar, or a separate dialogue box. The intricacies of linkages must also be known to them. Sometimes a button, picture, or phrase such as "click here" might disguise the right place. The exact location is frequently concealed unless someone knows where to search. In certain odd instances, the URL is shown in its entirety. The tooltip provided is probably an attempt to fool clients into believing they are secure.

4.2 Determine the URL's So-Called Who-Area:

Once the actual target URL has been determined, individuals should discover the domain, also known as who-area. These are the final two words in the URL that have been separated by a dot before the initial "/," as stated in the video.

We caution that phishers fool users by placing the name of the genuine company instead of the who-area in the URL. It might be put before or behind the who-area. You should not depend on the HTTPS signal. Here are a few such phishing URLs:

https://www.gmail.com.mail-nows.com/login
https://mail-nows.com/https://www.gmail.com/login.

4.3 Verify the Who-Authenticity: Area's

After you have determined the who-area, the last step is to verify that each character must be passed on one at a time. Phisher usually uses (1) trustworthy phrases in the who are (for example, 'secure-shop.com') and (2) invisibly changes the characters. It may, for example, replace a 'd' with a 'cI' or produce mistakes such as 'Micrоsoft.'

We've collaborated with someone who creates awareness films to create a shop and voice-over script based on the message content. We utilized basic, non-technical phrases and languages (for example, the word "who-area" for domain). We have marked screenshots to assist you in identifying important information (e.g., the status bar). We asked for opinions from individuals of all ages and backgrounds with diverse degrees of IT and security to help us construct and refine the movie. A professional film manufacturer utilized our information and experience to create the video. The comments from numerous representatives of the targeted audience enhanced the film.

5. Case Study Of Awareness Programs Among Student

For many years, protecting yourself online has been crucial. The number of virtual assaults on computers has increased directly and indirectly. For future employees to have the extra cybersecurity abilities to correctly safeguard the country's interests, pupils must be trained in the network's safety issues. An overwhelming quantity of rules to learn, making it difficult for youngsters to participate completely. Players need a decent understanding of cybersecurity to play some of the top cybersecurity games. Several instructional computer games are targeted by high school students. However, just a few games have been designed to help university students learn more about safety. In addition, several educational game producers have given great emphasis to research and development. They didn't devote enough attention to the game review and assessment.

5.1. Background of Student

We have maintained our learning goal to educate young people effectively on fundamental cybersecurity concepts during our research and development. Our success was judged by how effectively persons inexperienced with cybersecurity could understand the information offered in the game. They also examined the ability of players to answer questions in the games based only on what they had learned while playing. For future research, we decide to preserve a data log to evaluate the success of the game. We tested it in courses. Explore how the game impacts students in various settings.

5.2. Population and Community

a. Evaluation In Major Courses In Computer Science And Information Technology

A comparison of pre-and post-test data was the beginning point for the impact study. We invited both groups to reply to five questions on phishing worth two points each. We asked them to do this. Then the youngsters finished the game from start to finish. The kids did a post-game assessment comparable to the pre-game evaluation. We evaluated the findings to see whether overall performance had improved. Eight out of 11 students in the CSC1310 group improved their qualifications. These people have made improvements between 20% and 80%, with an average of 37.5%. Three other kids scored more reassuringly since they were consistent: one young person received 8 points on both occasions, and the other two got a perfect ten. Fig. 9 shows pre-test and post-test scores of CSC1310 (a). Table I summarizes the findings of the test assessment for this group. The average score before the test was 5.3. However, after the trial, the average score was 8. The two-tailed t-test results are 0.0056, showing a statistically significant difference between pre-and post-test.

For the CSC3332 group, we gathered the same information. Twelve of the 19 students increased their scores in the cohort. The improvements ranged from 20% to 80%, with these participants rising by an average of 20%. Five out of 19 children each received the same score, one eight and four achieving the perfect 10. Unfortunately, three student scores plummeted 20 percent despite several attempts. This group's performance was compared before and after the test in Figure 9. (b). Table I also summarizes this group's test evaluation. The average before the exam was 7.7. However, after testing, the standard was 8.7. The p-value of the two-tail t-test paired is 0.037, revealing a significant rise from before to after the test.

5.3. Feedback From The Student About The Game

According to the pre-test and post-test comparisons in Table I, the CSC1310 group's post-test average increased by 51 percent. On the other hand, the average CSC3332 group only grew by 13 percent. We saw that the outcomes matched our expectations. Because the CSC1310 group contained largely freshmen who may not have had a lot of exposure to phishing before playing the game, their average increased significantly. The CSC3332 class is, on the other hand, a junior computer science class. Therefore they knew security well before the game. Because the average pre-test was so high, we were delighted to see this group rise 13%.

Besides the pre-and post-test comparison, we reviewed the log files meticulously. Each log file tracks the number of efforts a pupil requires to undergo level 3. We can observe that numerous players needed more than three games to get a score in CSC1310. Eighty percent of athletes require 3 to 5 tries, with one outlier of 9. On the other hand, the majority just needed one or two tests, demonstrating that the use of the game is an effective teaching technique. The summary of the log files for both courses is shown in Table II. No participant needed more than three CSC3332 attempts. This indicates that the game has an easy learning curve for those with little or no previous understanding of its ideas. In addition, 15 of the 19 participants (79 percent) needed only two playthroughs to achieve a passing grade.

b. Non-CS/IT majors are evaluated in non-CS/IT major courses.

In spring 2018, we utilized the game in five sessions of CSC1306 (Computer and its Use I) to examine how students with no previous computer expertise were impacted. It is considered a general education course for non-CS/IT major students to meet information literacy. The course covers everything from digital computers to software applications, I/O devices, storage devices, software systems, software assessment, and computer ethics.

For the start of the impact research, a comparison of pre-and post-test data was employed. Students must complete the pre-test before the game starts. Students took a post-test after the main games that were similar to the pre-test. The review comprises five questions worth two points each. The two results were then compared to discover whether general performance variations existed. The 70 competitors consisted of 38 women and 32 men. Figure 10 shows the pre-and post-test performance of this group. Accordingly, 67 percent of students improved the outcomes of pre-and post-test comparisons in Table III, more than the 51 percent improvement indicated in the first CSC1310 study. Students have a pre-test average of six. In the post-test, this figure jumped to 8.4. Finally, the p-value of the t-test pairing with two tails is 3.328E-9, which suggests a statistically significant difference between pre-and post-test.

In addition to the comparison before and after testing, we have looked at the log files in detail. Each log file tracks how often a student has to try to pass Level 3. For each group, a passing score required at least one replay and at least five playthroughs. 41.43% of students finished level 3 on their first attempt, 32.86% were successful in their second attempt, and 25.71% succeeded in three or more tries. Most of the participants (90 percent) required just one or three tests to show that the game could be used as a tool to educate. Table IV provides the CSC1306 group log file summary.

These evaluation findings show that the game's themes had a beneficial influence on players' comprehension of phishing. The majority of pupils took around 20 minutes to do the work (pre-test, competition, post-test, and survey). According to a comparison of 100 participants before and after the exam, the game had a favorable influence on students' understanding of phishing tactics.

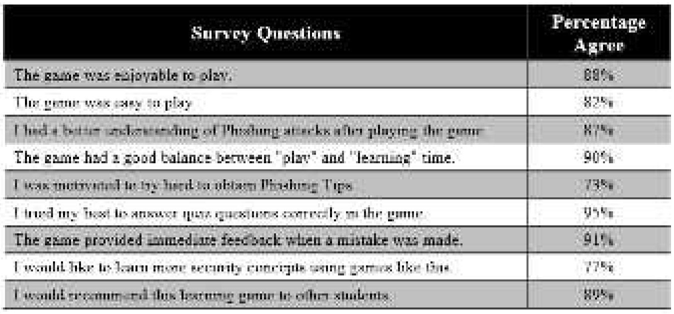
6. Result From The Awareness Program

When the experiment was completed, an illustrated website was created to explain the investigation facts, analyze the data, educate readers on what a phishing attack is, and how they may avoid becoming victims in the future. All AUS users were advertised on the website, and it was also publicized in the local news. Two weeks later, a second phishing audit was conducted to examine the success of sensitivity exercises. Surprisingly, the audit touched just 220 individuals, all students. The number of victims in the second audit decreased from 9% to 2%, which shows that awareness training was successful.

7. Debate Discussion

Each group had the option of expressing comments and criticism about the game as a whole anonymously. This was quite useful to lead us to a better quality gaming experience. One of the most common suggestions during the evaluation of the game was to clarify the instructions for "How to Play." In particular, the bomb launch mechanism of stage three proved difficult to grasp for many gamers. We addressed this by changing the instructions for moving the bomb to show that scrolling is necessary for launching. We also have a boss-level request that we are reviewing.

The game has been improved in response to the comments of the youngsters. In addition to these ideas, most of the answers simply congratulated us for a well-designed game and remarked that the recommendations were beneficial to understand how to resist phishing. Table V summarises the survey findings that 138 students completed.



Survey Questions	Percentage Agree
The game was enjoyable to play.	88%
The game was easy to play	82%
I had a better understanding of Phishing attacks after playing the game	87%
The game had a good balance between "play" and "learning" time.	90%
I was motivated to try hard to obtain Phishing Tips	73%
I tried my best to answer quiz questions correctly in the game.	95%
The game provided immediate feedback when a mistake was made.	91%
I would like to learn more security concepts using games like this.	77%
I would recommend this learning game to other students.	89%

Table 1: Survey Results

8. Acknowledgement

The authors would like to thank all School of Computing members who were involved in this study. This study was conducted for the purpose of the System and Network Security Research Project. This work was supported by Universiti Utara Malaysia.

References

Dixson, D. D., & Worrell, F. C. (2016). Formative and summative assessment in the classroom. *Theory into Practice, 55*(2), 153-159.

Dolin, J., Black, P., Harlen, W., & Tiberghien, A. (2018). Exploring Relations between Formative and Summative Assessment *Transforming Assessment* (pp. 53-80): Springer.

Harlen, W., & James, M. (1997). Assessment and learning: differences and relationships between formative and summative assessment. *Assessment in Education: Principles, Policy & Practice, 4*(3), 365-379.

Iannone, P., & Simpson, A. (2017). University students' perceptions of summative assessment: The role of context. *Journal of Further and Higher Education, 41*(6), 785-801.