An Evaluation of User Awareness for the Detection of Phishing Emails

Mohammed I Alwanain
Department of Computer Science,
College of Science and Humanities in Alghat
Majmaah University
Saudi Arabia

***Abstract*—Phishing attacks are among the most serious Internet criminal activities. They aim to make Internet users believe that they are using a trusted entity, for the purpose of stealing sensitive information, such as bank account or credit card information. Phishing costs Internet users millions of dollars each year. An effective method that can prevent such attacks is improving the security awareness of Internet users, especially in light of the significant growth of online services. This paper discusses a real-world experiment, which aims to analyze and monitor the phishing awareness of an organization's users in order to improve their awareness. The experiments have been targeting 1500 users in the education sector. The results of the experiment reveal that phishing awareness has a significant positive effect on users' ability to distinguish phishing emails and websites, thereby avoiding attacks.**

Keywords*—Anti-phishing countermeasures; online fraud; evaluation experiments

I. INTRODUCTION

E-commerce and online services make our lives more comfortable and manageable, wherever we may be and at any time of day. However, this ubiquity of service carries with it a critical security threat, which can cost Internet users dearly. One such threat is posed by phishing, whereby a criminal (phisher) will attempt to steal a user's sensitive information (such as credit and debit card details, bank account details, and address) using fake emails, fake websites, or both [1]. Therefore, phishing attacks have become one of the most serious types of threat to businesses and the public in recent years [2]. According to the Canadian Center for Cyber Security [3], the number of reported phishing attacks is around 156 million emails per day, and the number of victims reaches around 80,000 per day. Alsadoon [4] stated that the target of these attacks is the financial sector, which received 70% of the reported attacks in the third quarter of 2018 [5]. For instance, in 2005, the Bank of America lost 1.2 million usernames and social security numbers (SSNs) belonging to its customers, which led to the loss of millions of dollars. In 2011, the details of 10 million credit cards belonging to users were stolen from Sony Entertainments, which cost approximately two billion dollars, making it the most expensive cyber-hack in history [2]. The FBI's Internet Crime Report for 2017 counts phishing attacks amongst the top three types of crime cited by victims of Internet crime, with losses of approximately 30 million dollars being recorded for that year. In fact, this number is likely to be much higher because not all attacks are reported.

The financial sector is not the only target for phishers; a Malcovery report for the last quarter of 2013 showed that the top five organizations targeted by phishers were Facebook, WhatsApp, UPS, Wells Fargo, and Companies House (UK) [6], indicating that phishing attacks target people's social lives as well as their financial interests. Consequently, both industry and academia are working hard to develop solutions to the phishing threat. It is therefore of paramount importance that organizations pay attention to end user awareness when attempting to prevent phishing.

Phishing is a very hard security issue to prevent for two main reasons. First, it is very easy for the phisher to design an identical website that represents a bank or famous brand and looks very convincing to users, so that a significant percentage of users are unable to recognize a phishing attack. Second, most phishing attacks are currently hosted on websites that have HTTPS and SSL certificates.

Recently, a number of technical solutions have been proposed to mitigate the problem of phishing, such as SpoofStick, Netcraft, and SpoofGuard. However, these tools are not the only means developed to prevent attacks [7]. For instance, Dhamija et al. [8] conducted a phishing experiment, with results that revealed how 23% of the study participants never looked at the address bar or status bar when receiving a link by email and did not even understand the anti-phishing tool indicators. This led them to making mistakes in the experiment 40% of the time and these mistakes were the main reasons for phishing attacks. That study demonstrated that anti-phishing training for end users should be mandatory for any technical solution proposed. According to Symantec[9], users' awareness is central to changing their behavior and preventing online scams. A higher level of awareness will reduce the number of mistakes made by users when dealing with phishing emails and websites.

In [10], we conducted two phishing experiments, each was written in a different language (English and Arabic). We found that the number of participants who failed to detect the phishing email in the first experiment was sharply reduced in the second experiment, for two reasons. The first reason was the improvement in the participants' phishing awareness, due to phishing information that we provided to the victims when they clicked the link. The second reason was the language of the email. Although the majority of the participants were non-English speakers, the second experiment was conducted in

English. Consequently, we found that the language of the email also has a significant effect on the results of experiments. In this paper, we conducted a phishing experiment, Which is an extension of the experiments in [10]. The aim of this experiment is to evaluate the improvement on user's awareness when the email is written in two different languages (Arabic and English in this experiment) and to compare the result of this experiment with the experiments presented in [10], both of which have been carried out in the same environment. Moreover, the experiment in this paper has been conducted in real-world environment. The sample in this experiment consists of the victims who clicked on the phishing link in both experiments mentioned above (which was presented in a previous paper [10]), as well as a new group of participants. Furthermore, the new experiment was conducted in an educational context, with the aim of studying the outcomes produced by participants who comprised computer science specialists and faculty members with a PhD in computer security. The results of the experiments outlined in this paper strongly support the assumption presented above: that technical solutions cannot prevent phishing attacks without user awareness.

The remainder of this paper is organized as follows. Section two presents the background literature on anti-phishing approaches. In section three, the research hypotheses are described, while the fourth section explains the research methodology. The fifth section defines the evaluation method implemented. In the sixth section, the results of the experiment are presented, and the paper is then concluded with a discussion of the findings and recommendations for future work.

II. Related Work

Security issues in technology have been recognized since technology became very significant in all aspects of human life. For instance, in 1960, access controls and encryption approaches were developed to protect passwords from a security threat known as "phone phreaking." At the time, phone phreaking referred to the use of an electronic device called a "blue box," which was capable of emitting the frequencies used by telephone companies, thereby making it possible to make free calls. The "ph" in "phishing" is derived from this term, with "ph" replacing the "f" in "fishing" [1].

The term "phishing" was first used in 1996, when hackers stole users' confidential information from America On-line (AOL) [1], [2]. In that incident, the hackers contacted AOL users via fake emails and asked them to verify their passwords for security purposes. As a result, many users provided passwords to the hackers, who were then able to make purchases from their accounts. This ultimately cost millions of dollars at the expense of legitimate users. According to [11], the main domains targeted by hackers for phishing are .com, at 41%, followed by .net at 7%, .org at 5%, and .br at 3%.

In recent years, there have been numerous attempts to reduce the incidence of phishing: for example, through the introduction of anti-phishing toolbars, which are Web browser plug-ins that warn users when they access a suspected phishing site [12]. Additionally, many financial, commercial, private, and government institutions (for example, eBay and HSBC) offer guidance on how to prevent phishing. The aim of these tips is to train users to look for signs of phishing in emails and websites, thereby enabling them to identify phishing attempts more effectively. In general, however, ordinary users do not read the online material intended as anti-phishing training, even though this can be effective if applied [13].

In contrast, Sheng et al. [14] proposed an online game to teach users good habits, helping them to avoid phishing attacks. Kumaraguru et al. [15] also considered training users to identify and deal with phishing emails during their everyday email use. Their aim was to teach users to look for phishing clues in their emails. They found that this training approach works better than the current practice of sending anti-phishing tips by email. However, the above approach did not include teaching users how to avoid phishing websites.

There are various ways in which phishing sites may be accessed, such as in online advertisements. Alnajim and Munro [16] proposed an anti-phishing strategy in the form of a training intervention. This is designed to help users ascertain whether a website is legitimate. It provides information for end users and helps them as soon as they make a mistake. The above authors found a positive effect of using their approach, compared with the earlier strategy of sending anti-phishing tips by email.

The approaches of Kumaraguru et al. [15] and Sheng et al. [14] were evaluated in studies involving participants who had been recruited on the basis of their technical background. Prospective participants were classified as either "expert" and "non-expert" users, based on pre-study screening questions. Their technical background was judged according to whether they had ever changed preferences or settings in their Web browsers, created a Web page, or helped someone to resolve a computer problem. Any participant who answered 'No' to at least two of the screening questions was selected to take part in the experiments. This assessment of technical background was therefore used to recruit non-experts. However, these apparent non-experts in the use of the relevant technology may have already been aware of phishing and how to detect attacks, before taking part in the evaluation experiments, leading to biased results. This is because participants with prior knowledge of phishing may have applied their existing knowledge, rather than the anti-phishing approaches being taught in the experiment.

Fettel et al. [17] proposed machine learning methods to detect a phishing attack. These approaches assessed the properties of URLs contained within an email (for example, the number of dots in the URL, the age of the linked domains, and the number of links in the email) to flag emails as phishing emails. These techniques are helpful in filtering phishing emails but still cannot prevent the attacks without an improvement in the user's knowledge of phishing.

Downs et al. [18] studied whether there was any correlation between a level of experience of the Web environment and susceptibility to phishing. They found that users who correctly answered a question about the definition of phishing (that is, phishing-aware users) were significantly less likely to be deceived by phishing emails.

A similar approach has been proposed by Alnajim [19]. The model presented was mainly a prototype of an automated analyzer for users' anti-phishing behavior within a LAN. This analyzer automatically performs ongoing analysis of users' behavior in response to phishing attacks. Based on the results of this analysis, the analyzer decides whether users require training in the detection and avoidance of phishing. However, this approach goes beyond that by adding an advanced setting that fully automates the training without the human intervention. This approach has been implemented and evaluated in a real-world context.

In [10], we conducted two different phishing experiments, targeting active users who were randomly selected from different specialties and who had different levels of knowledge. In the first experiment (Experiment 1), a phishing email (in Arabic) was sent from an unofficial domain to 1500 active users, who used email regularly in the education sector. This email was written in Arabic because most Internet users at the university (87%) were Arabic speakers. The sample included managers, faculty staff, and general employees. The phishing email was designed to resemble a legitimate email, requesting users to update their passwords immediately via a website link. The hyperlink directed the users to a website that informed the users that they had been targeted by a phishing email. The website consisted of information about phishing and the most common phishing scenarios, with the aim of improving users' knowledge and thereby avoiding any future phishing attacks. In the second experiment (Experiment 2), an English version of the same email was sent to a sample of the same size, consisting of users who had failed to detect the phishing email in Experiment 1, as well as some new participants who had not participated in the first experiment. The email in the second experiment was in English, to evaluate the awareness of non-Arabic speaking participants and the curiosity of non-English speaking participants. The results revealed that a significant improvement was identified in the phishing awareness of those who had participated in the first experiment: only five participants from Experiment 1 clicked on the link. In this paper, we continue examining participant awareness by conducting an experiment evaluating the user's awareness when the email written in two different languages that can be understand by all the users. The following sections describe this technique in detail.

III. Research Hypotheses

With this approach, the research hypotheses can be expressed as follows:

Hypothesis 1: There is no significant impact of the language of the email in recognizing and detecting Phishing email.

Hypothesis 2: The time of sending the phishing email has a significant impact. The majority of the victims are always affected by phishing on the first day, but the rate dropped sharply over subsequent days.

An evaluation and analysis of these hypotheses are presented in following sections.

IV. Implementation

A. Objective

Many public and private sector organizations, such as companies and universities, have many users in their local network. Those users use the organization's network to perform their required tasks, such as serving the public or students. Such tasks may require them to connect to the Internet to provide the organization's services online or to communicate with others. They may be exposed to phishing attacks because they are connected to the Internet. Consequently, improving the users' awareness of phishing attacks is a significant step toward preventing it.

B. Development

The website used in the experiment has been implemented in PHP Laravel, which is operated and stored on a local machine and run by an Apache server. The Domain Name System (DNS) host files in the Windows operating system were modified, so that the Web browsers displayed the URL of the actual phishing websites. When a user click on the corresponding link, the website would store information of importance to the experiment, such as the user's position, department, specialty, gender, IP address (to see if he or she was accessing the site from within or outside the domain), date, and time. All this information was stored in the local database, so that a statistical analysis could be carried out.

V. Methodology

The experiment presented in this paper has been conducted in a real-world context, to produce results that are close to reality which was the main goal of the approach.

In this experiment, the phishing email was written in Arabic and English, and was sent from an unofficial domain to 1500 active users who used email regularly in the education sector. The sample included managers, faculty staff, and general employees. However, students fell outside the scope of this study. The sample also included the victims who had clicked the phishing link in Experiments 1 and 2 of [10].

The phishing email was designed to resemble a legitimate email, informing the users that their mailboxes had reached the limit and encouraging them to increase the size by clicking on a given link.

The hyperlink attached to the button directed the users to a website, which informed the users that they had been targeted by a phishing email. The website consisted of information about phishing and the most common phishing scenarios, with the aim of improving users' knowledge and thereby avoiding any future phishing attacks. In this paper, it was assumed that a participant clicking on the hyperlink would become a phishing victim.

VI. Results

Once the experiments had been completed, a statistical analysis was carried out using IBM SPSS Statistics. In the experiment, the emails were sent to local active users. This involved filtering the users and eliminating those who had not used their email accounts for at least a month. This kind of filtering was very useful for determining the accuracy of the

results, ensuring that only active users were involved in the study. In the experiments, we analyzed the results with respect to the users' confidentiality and privacy. The following sections describe these experiments in detail.

A. Experiment

In the experiment, the email was sent to 900 (60 %) male users and 600 (40%) female users over a period of three days: from December 5–8, 2018. As mentioned above, the email was in Arabic and English, to cover both Arabic and non-Arabic participants. The results of the experiment showed that the total number of users who opened the email amounted to 580: 287 female and 293 male.

192 participants clicked on the link. Similar to the previous experiments, the highest rate at which participants became victims happened on December 5 (57.3%) and the lowest rate was 0.5%, which happened at the end of the experiment. As mentioned in [10], this was because of some users who were more aware, users with a technical background, and the first victims to suffer attacks warning other users about the phishing emails via social media, such as WhatsApp.

In terms of gender, 63% male and 37% female participated, where only 36 of the males and 14 females were PhD holders. The majority of participants (68.8%) were employees, followed by faculty (26.6%), managers (4.2%), and deans (0.5%) (see Table I).

Further analysis was carried out to determine the relationship between gender, position, PhD status, and date (see Table II). The results show a weak negative correlation between date and position (r=-0.157, N=192, P=0.030) and between date and PhD status (r=-0.158, N=192, P=0.029), which indicate that people with high position and PhD holders were less likely to become victims.

B. Results Comparison

This section discusses and compares the results found in the new experiment (which we call Experiment 3) and the results of the experiments conducted in [10]. The total number of victims in Experiment 3 was 192 during three days, compared with 79 victims in Experiment 1 and 127 victims in Experiment 2 (see Table III). It was noticed from the three experiments that the number of the victims increased.

TABLE. I. DISTRIBUTION OF SAMPLE ACCORDING TO PHD STATUS AND JOB LEVEL

Gender	**PhD holder**			
	No		**Yes**	
	Position		**Position**	
	Employee	**Manager**	**Dean**	**Faculty**
Female	54	1	0	14
Male	77	7	1	35
Total	131	8	1	49

TABLE. II. PEARSON CORRELATION MATRIX.

		Gender	**Date**	**position**	**PhD holder**
Gender	Pearson Correlation	1	.007	.092	.119
	Sig.(2tailed)	.000	.920	.202	.101
	N	192	192	192	192
Date	Pearson Correlation	.007	1	-.157-[a]	-.158-[a]
	Sig.(2tailed)	.920	.000	.030	.029
	N	192	192	192	192
position	Pearson Correlation	.092	-.157-[a]	1	.947[b]
	Sig.(2tailed)	.202	.030	.000	.000
	N	192	192	192	192
PhD holder	Pearson Correlation	.119	-.158-[a]	.947[b]	1
	Sig.(2tailed)	.101	.029	.000	0
	N	192	192	192	192

[a] Correlation is significant at the 0.05 level (2-tailed).

[b] Correlation is significant at the 0.01 level (2-tailed).

TABLE. III. DISTRIBUTION OF SAMPLES ACCORDING TO THE EXPERIMENT, AND WHETHER A SPECIALIST OR PHD HOLDER

					PhD holder			
					No		**Yes**	
					Employee	**manager**	**Dean**	**faculty**
Group	Experiment1	female	Specialist	No	11	0	0	1
				Yes	1	2	0	0
		male	Specialist	No	35	3	1	12
				Yes	8	3	2	0
	Total				79			
	Experiment2	female	Specialist	No	17	0	1	12
				Yes	2	0	0	2
		male	Specialist	No	43	3	2	37
				Yes	7	0	1	0
	Total				127			
	Experiment3	female	Specialist	No	53	0	0	14
				Yes	1	1	0	0
		male	Specialist	No	72	5	1	35
				Yes	5	2	0	0
	Total				192			

This is because, in each experiment, a new phishing email was sent using a different email style, and it was also written in different languages. However, the number of users who failed to detect the phishing email decreased from 79 victims in Experiment 1 to five victims in Experiment 2. In addition, the victims of Experiments 1 and 2 were involved in Experiment 3 and the results show that only 12 users out of 84 (the sum of the victims of Experiments 1 and 2) clicked on the link, as Fig. 1 shows.

The third experiment has the largest number of victims. This is because the email was written in English and Arabic, so both Arabic and non-Arabic speakers were among the participants because they understand the content of the email. In Experiment 3 there was a weak negative correlation between date and position of message opening (r=-0.157, N=192, P=0.030), compared with a non-significant correlation between date and position in the result of Experiment 1 and Experiment 2, as Table II shows.

VII. Discussion

From the experiments presented in this paper and in [10], the results clearly showed a high and significant effect on users' phishing awareness, demonstrated by users correctly identifying a phishing email and thereby avoiding a phishing attack. As a result, this led to a higher rate of phishing avoidance amongst phishing-aware users, compared with the less aware users. This appeared in a comparison between the results of the three experiments presented in the previous section, with the difference between them indicating a significant positive effect of phishing awareness, as compared with low phishing awareness. Consequently, it would appear that the awareness of phishing has a significant positive effect on users' ability to detect and therefore prevent phishing.

In addition, it was clear from the experiments that having a technical background had little effect on users' ability to distinguish between phishing and legitimate emails. However, this study demonstrated that, in comparison with users who had less awareness of phishing, there was a significant positive effect of phishing awareness on phishing detection.

The results also show that the language of the email has a significant impact. For instance, the experiment presented above has a larger number of victims than the experiments presented in [10]. Consequently, Hypothesis 1 is rejected. This is because the email used in the third experiment was written in Arabic and English, so both Arabic and non-Arabic speakers can participate.

Another significant finding was that the majority of the victims were affected by phishing on the first day of each experiment, but the rate dropped sharply over subsequent days. Hypothesis 2 is therefore accepted, because of some users who were more aware, users with a technical background, and the first victims to suffer attacks warning other users about the phishing emails via social media networks, such as WhatsApp.

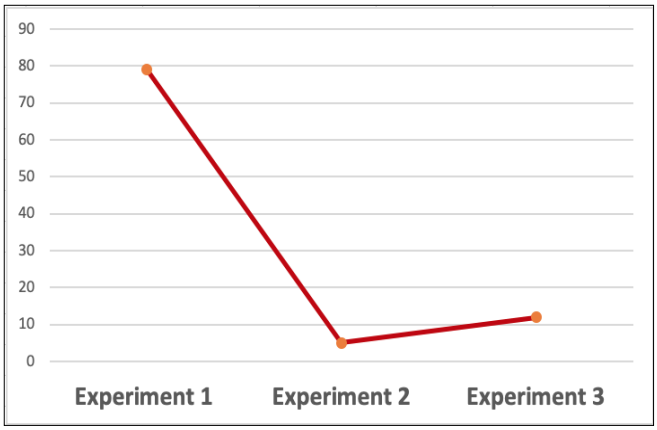

Fig. 1. Victims who Clicked on the Link in Two or All Experiments.

Additionally, Fig. 1 shows that the number of the victims who failed to detect the phishing email in Experiment 1 was reduced sharply in Experiment 2 and Experiment 3. This is because user awareness improved, and the users were able to detect the phishing email.

VIII. Conclusion

The aim of this paper was to demonstrate a phishing experiment which aimed to simulate, analyze and monitor the phishing awareness of users to improve it. This experiment was conducted on a sample of users in a real environment, and the results were reported and interpreted. Significant positive effects were found, with regard to the ability of users to determine whether emails were legitimate or designed solely for the purpose of phishing. The paper also presented a comparison between the result of the experiment conducted in this paper and the related results presented in [10]. Furthermore, the experiments revealed a pressing need for practical training to enhance phishing awareness.

Future work will involve a phishing experiment on students of Computer Science, with a particular focus on security students. The aim being to evaluate the impact of modules dedicated to the topic of security, on the student' own security awareness.

Acknowledgment

The author would like to thank Deanship of Scientific Research, Majmaah University (Grant no. R-1441-5) for funding this work.

References

[1] Gupta, N. Arachchilage, and K. Psannis, "Defending against phishing attacks: taxonomy of methods, current issues and future directions," Telecommun. Syst., vol. 67, no. 2, pp. 247–267, 2018.

[2] A. K. Jain and B. B. Gupta, "Phishing detection: analysis of visual similarity based approaches," Secur. Commun. Networks, vol. 2017, no. 5421046, 2017.

[3] Canadian Centre for Cyber Security, "Phishing: How many take the bait," 2015. [Online]. Available: https://www.getcybersafe.gc.ca/cnt/rsrcs/nfgrphcs/nfgrphcs-2012-10-11-en.aspx.

[4] I. Alseadoon, "The impact of users' characteristics on their ability to detect phishing emails," Queensland University of Technology, 2014.

[5] Anti-Phishing Working Group, "Phishing Activity Trends Report. 3rd Quarter 2018," 2018.

[6] S. Ragan, "Senior executives blamed for a majority of undisclosed security incidents," 2013. [Online]. Available: http://www.networkworld .com/article/2171678/data-center/senior-executives-blamed-for-a-majority-ofundisclosed-%0Dsecurity-incidents.html.

[7] A. Alnajim, "A country based model towards phishing detection enhancement," Int. J. Innov. Technol. Explor. Eng., vol. 5, no. 1, pp. 52–57, 2015.

[8] R. Dhamija, J. D. Tygar, and M. Hearst, "Why phishing works," in the SIGCHI conference on Human Factors in computing systems, 2006, pp. 581–590.

[9] "Symantec, Mitigating Online Fraud: Customer Confidence, Brand Protection, and Loss Minimization.," 2004. [Online]. Available: http://www.antiphishing.org/sponsors_technical_papers/symantec_online_fraud.pdf.

[10] M. Alwanain, "Effects of User-Awareness on the Detection of Phishing Emails: A Case Study," Int. J. Innov. Technol. Explor. Eng., vol. 8, no. 4, pp. 480–484, 2019.

[11] IID, "eCrime Trends Report." [Online]. Available: http://internetidentity .com/resources.

[12] L. F. Cranor, S. Egelman, J. I. Hong, and Y. Zhang, "Phinding Phish: An Evaluation of Anti-Phishing Toolbars," 2006.

[13] A. Alnajim and M. Munro, "An evaluation of users' tips effectiveness for Phishing websites detection," in The third IEEE International Conference on Digital Information Management ICDIM, 2008, pp. 63–68.

[14] S. Sheng, B. Magnien, A. Kumaraguru, Ponnurangam Acquisti, L. F. Cranor, and J. Hong, and E. Nunge, "Anti-phishing phil: the design and evaluation of a game that teaches people not to fall for phish," in The 3rd symposium on usable privacy and security SOUPS '07, 2007, pp. 88 – 99.

[15] P. Kumaraguru, Y. Rhee, A. Acquisti, L. F. Cranor, J. Hong, and E. Nunge, "Protecting people from phishing: the design and evaluation of an embedded training email system," in The SIGCHI conference on Human factors in computing systems, 2007, pp. 905 – 914.

[16] A. Alnajim and M. Munro, "An anti-phishing approach that uses training intervention for phishing websites detection," in the 6th IEEE International Conference on Information Technology - New Generations (ITNG), 2009, pp. 405–410.

[17] I. Fette, N. Sadeh, and A. Tomasic, "Learning to detect phishing emails," in Proceedings of the 16th international conference on World Wide Web, 2007, pp. 649–656.

[18] J. S. Downs, M. Holbrook, and L. F. Cranor, "Behavioral response to phishing risk," in the anti-phishing working groups 2nd annual eCrime researchers summit, 2007, pp. 37 – 44.

[19] A. Alnajim, "An Automated Analyzer for Users' Anti-Phishing Behaviour within a LAN," Int. J. Soft Comput. Eng., vol. 5, no. 3, pp. 115–119, 2015.