International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-8 Issue-4, February 2019

Effects of User-Awareness on the Detection of Phishing Emails: A Case Study

Mohammed I. Alwanain

Abstract*: *In recent years, most of our daily services have been increasingly linked to the Internet, such as online banking and online shopping, thereby making our lives more comfortable and manageable, wherever we may be and at any time of day. However, this ubiquity of service also carries a critical security threat, which can cost Internet users dearly. Therefore, improving Internet users' security awareness is a matter of high importance, especially in light of the significant growth of online services. This paper investigates the effects of security awareness and phishing knowledge on users' ability to detect phishing emails and websites. In this approach, two experiments were conducted to evaluate the effects of security awareness. The results of these experiments revealed that phishing awareness has a significant positive effect on users' ability to distinguish phishing emails and websites, thereby avoiding attacks.

Index Terms*: *Anti-phishing countermeasures, online fraud, E-commerce security, online banking security, evaluation experiments

I. INTRODUCTION

Due to the growth of Internet technology, online services face serious security threats to their systems and networks. One such threat is posed by 'phishing', whereby a phisher will attempt to steal a user's sensitive information (such as credit and debit card details, phone numbers and addresses), 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]. 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. Then, 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[3]. However, personal banking details are 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)[4], 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.

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[5]. For instance, Dhamija et al.[6] conducted a phishing experiment, with results that revealed how 23% of the study participants never looked at the address bar or bar status on receiving a link by email and did not even understand the anti-phishing tool indicators. This led to them making mistakes in the experiment 40% of the time and these mistakes were the main reasons for phishing attacks. It demonstrated that anti-phishing training for end-users should be mandatory in any technical solution proposed. According to Symantec[7], users' awareness is central to helping change their behaviors and prevent online scams. A higher level of awareness will reduce the number of mistakes made by users when dealing with phishing emails and websites.

In this paper, two experiments are reported. They involve phishing attacks in a real environment, for the purpose of evaluating users' reactions when attacks occur. The results of the experiments outlined in this paper strongly support the assumption presented above, namely 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 methods implemented. In the sixth section, the results of the two experiments are presented and the paper is then concluded with a discussion of the findings and recommendations for future work.

II. RELATED WORK

From the early '60s, the security of technology has emerged as a serious issue. For instance, in 1960, certain access controls and encryption approaches were developed to protect passwords from a security threat known as 'phone phreaking' [1]. At the time, phone phreaking referred to an electronic device called a 'blue box', which was capable of emitting the same frequencies as telephone companies and thereby rendering 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.

Manuscript published on 28 February 2019.
***Correspondence Author(s)
Dr. Mohammed I. Alwanain, Department of Computer Science, Majmaah University, Majmaah, Saudi Arabia.

As a result, many users provided the hackers with their passwords, who were then able to make purchases from their accounts.

This ultimately cost millions of dollars at the expense of legitimate users. According to eCrime Trends Report [8], the main domains targeted by hackers for phishing are .com, at 41%, followed by .net at 7%, .org at 5%, and .br at 3%.

However, 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 [9]. 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 [10].

In contrast, Sheng et al.[11] proposed an online game to teach users good habits, thus helping them avoid phishing attacks. In addition, Kumaraguru et al.[12] 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.

In addition, there are various ways in which phishing sites may be accessed, such as in online advertisements, wherein Alnajim and Munro[13] propose an anti-phishing strategy in the form of a training intervention. This is designed to help users ascertain whether or not a website is legitimate. It provides information for end-users and also helps them as soon as they make a mistake. The above authors found a positive effect of using their approach, compared to the earlier strategy of sending anti-phishing tips by email.

Kumaraguru et al. [12] and Sheng et al. [11] approaches were evaluated in studies involving participants who had been recruited on the basis of their technical background prospective participants were classified into '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 resolve a computer problem. Any participant who answered 'No' to at least two of the screening questions was selected to take part in the above-mentioned 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, thus 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.

Furthermore, Downs et al.[14] 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 knowledge question about the definition of phishing (i.e. phishing-aware users) were significantly less likely to be deceived by phishing emails.

Although there are clear advantages to filtering phishing attacks at email and website level, these approaches cannot prevent spam email. In this paper, we report on the evaluation of users' knowledge in a real environment, in order to discover how they interact with phishing emails. We therefore conducted two different phishing experiments; targeting active users, who were randomly selected from different specialties and different level of knowledge. In these experiments, we analyzed the results with respect to the users' confidentiality and privacy. The following sections describes these experiments in detail.

III. Research Hypotheses

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

Hypothesis 1: A significant improvement can be observed in the phishing awareness of the sample participating after the first experiment.

Hypothesis 2: No difference can be observed between participants who have attained a high educational level, and those who have not, as regards being able to differentiate between legitimate and phishing emails.

An evaluation and analysis of these hypotheses is presented in the following section.

IV. Methodology

The experiments presented in this paper were conducted in a real-world context, but most of the phishing experiments applied a 'role playing' protocol [5], [6], [11], [12], [13], due to the fact that conducting experiments in a real environment is likely to produce results that are close to reality, which is the main goal of the approach.

In this paper, two experiments were consequently executed. In the first (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 are Arabic speakers (87%). The sample included managers, faculty staff and general employees. However, students fell outside the scope of this study.

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, 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 (see Figure 1). In this paper, it was assumed that a participant clicking on the hyperlink became a phishing victim.

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 written in English, in order to evaluate the awareness of non-Arabic speaking participants and the curiosity of non-English speaking participants.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

Fig 1. A phishing website

V. IMPLEMENTATION

The websites used in these Experiments where 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 clicked 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 (see Figure 2).

VI. RESULTS

Once the experiments had been completed, a statistical analysis using IBM SPSS Statistics was carried out. In both Experiments, 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.

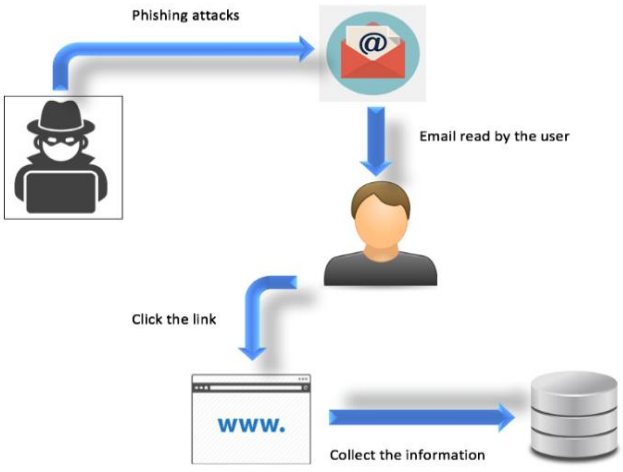

Fig 2. A phishing scenario

A. *Experiment 1*

In this Experiment, the email was sent to 800 (53.2%) male users and 700 (46.8%) female users over the span of three days; more specifically, from 7-9 December, 2017 (see Table 1). The results of the Experiment showed that the total number of users who opened the email amounted to 455: 150 female and 305 male. The majority (86.1%) were affected on the first day, whereas 10.1% were affected on the second day and just a small minority (3.8%) were affected on the third day.

Out of the users who clicked on the link, 79 (81%) were male (see Figure 3). Previous studies such as Sheng et al.[11] and Jagatic et al. [15] have shown that female users are more likely to become victims of phishing attacks than men. However, this Experiment yielded opposite results. Moreover, 15 of the male users held a Ph.D. and two were specialists in security. In contrast, only one female user with a Ph.D. became the victim of a phishing email.

Consequently, Hypothesis 2 is accepted, because a significant number of highly educated participants became phishing victims in the Experiment. This supports statistics that show how even security experts can fail to differentiate between phishing and real emails and websites [11], [15]. Aside from this, the majority of the participants in Experiment 1 were employees (69.6%), followed by faculty staff (16.5%), managers (10.1%) and Deans (3.8%) (see Table 1). However, this is to be expected, because there are fewer members of top-level management than there are employees.

Further analysis was carried out to determine the relationship between gender and date. The results revealed a weak negative relationship between gender and date with regard to opening the phishing email (r=-0.298, N=79, P=0.008), which is highly significant; indicating that the number of victims decreased according to the date (see Table 2).

In addition, there was a weak positive relationship between position and whether or not the participant held a Ph.D., and position and specialism (r=0.354, N=79, P=0.001), which is also highly significant; indicating that users with higher positions and a Ph.D. were more likely to be victims of phishing, as were users with high positions and a specialty in security.

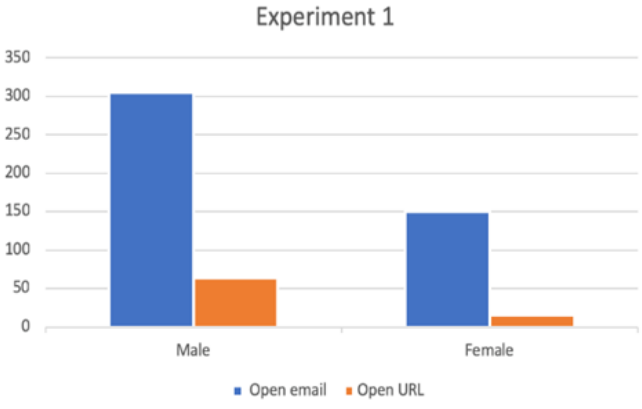

Fig 3. Total number of users by gender, who opened a phishing email and clicked on a link in Experiment 1

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

Table 1: Distribution of sample according to whether or not a Ph.D. holder, and job level

Gender	Ph.D. Holder			
	No		Yes	
	Position		Position	
	Employee	Manager	Dean	Faculty
Female	12	2	0	1
Male	43	6	3	12
Total	55	8	3	13

B. Experiment 2

In Experiment 2, an English-language version of the phishing email in Experiment 1 was sent to the sample. The email was sent to a new group of participants, which included users who had failed to detect the phishing email in Experiment 1. It was disseminated over a span of three days, from 16-18 September, 2018. We deliberately conducted the second experiment nine months later to ensure that any phishing awareness of the users would have diminished since Experiment 1, enabling us to accurately evaluate their current awareness.

In this Experiment, 342 users opened the phishing email (22.8%) (see Figure 4): 234 male and 108 female users (see Figure 5). However, the total number of victims who clicked on the link amounted to 127 (see Figures 4, 5): 93 male and 35 female.

The results also revealed that only five participants from Experiment 1 clicked on the link. Hypothesis 1 is therefore accepted, because a significant improvement was identified in the phishing awareness of those who had participated in the first Experiment. In addition, similar to Experiment 1, the highest percentage of victims (17.3%) was recorded for the first day and the lowest, for the last day, with just one victim.

With regard to gender, 73.1% of the victims were male and 26.8% were female. Three male users holding a Ph.D. were among the victims: two with a Ph.D. in Computer Science and one who was not a computer specialist. In contrast, 16 of the female users held Ph.Ds., but just one of these Ph.Ds. was in Computer Science. This means that Hypothesis 2 is accepted, because both Experiments included victims with a high educational level, including participants with a background in Computer Science. Therefore, no significant difference was identified between those who had attained a high level of education (including security specialists) and those who had not, in terms of being able to identify legitimate emails as opposed to a phishing attack.

Table 2: Distribution of sample by date.

Date		Frequency	Percentage	Valid Percentage	Cumulative Percentage
Valid	07/12/17	68	86.1	86.1	86.1
	08/12/17	8	10.1	10.1	96.2
	09/12/17	3	3.8	3.8	100.0
	Total	79	100.0	100.0	

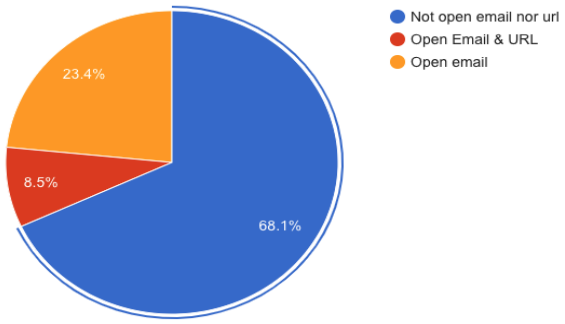

Fig 4. Total number of users who did/did not open the phishing emails and click on the link

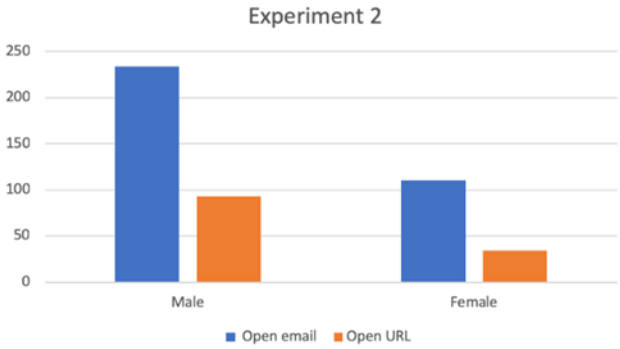

Fig 5. Total number of users by gender, who opened the phishing email and clicked on the link

Finally, the majority of the participants were general employees (54.3%), followed by faculty staff (40.2%), Deans (3.1%) and managers (2.4%) (see Table 3).

Further analysis was carried out to determine the relationship between gender and date. The results revealed a strong positive relationship between holding s Ph.D. and job position, and opening the phishing email (r=0.988, N=127, P=0.000), which is highly significant. It indicates that the participants with higher positions and a Ph.D. were more likely to be phishing victims. The results also showed a weak positive correlation between date and position, and date and the possession or otherwise of a Ph.D. (r=0.192, N=127, P=0.030 and r=0.179, N=127, P=0.044, respectively).

The results of Experiment 1 showed a highly significant weak negative relationship between gender and the date of opening the email (r=-0.298, N=79, P=0.008), which was not significant in Experiment 2.

Table 3. Distribution of sample whether or not a Ph.D. holder, and job level

Gender	Ph.D. holder			
	No		Yes	
	Position		Position	
	Employee	Manager	Dean	Faculty
Female	60	3	3	49
Male	9	0	1	2
Total	69	3	4	51

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

Meanwhile, in Experiment 1, there was a weak positive relationship between position and the possession or otherwise of a Ph.D., job position and specialty (r=0.354, N=79, P=0.001), which was highly significant. In contrast, in Experiment 2, there was a strong positive relationship between holding a Ph.D. and job position, and opening the phishing email (r=0.988, N=127, P=0.000).

VII. DISCUSSION

In the two Experiments described above, the results showed a significant effect on users' phishing awareness, demonstrated by users correctly identifying a phishing email and thereby avoiding a phishing attack. This led to a higher rate of phishing avoidance amongst the phishing-aware users, compared to the less aware users. This appeared in a comparison between the results of the two Experiments, with the difference between them indicating a significant positive effect of phishing awareness, as compared to 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 aforementioned Experiments that the fact of having a technical background had little effect on the 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.

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. This was due to 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. In addition, the findings illustrate that most of the victims were male in the two Experiments (81% in Experiment 1 and 73.1% in Experiment 2), whereas only 19% were female in Experiment 1 and 26.8% in Experiment 2. This deviates from Sheng et al.[11] and Jagatic et al. [15], where it was found that women were more likely than men to be victims of phishing.

Finally, the Experiments showed that even computer experts with a background in security could become victims of phishing attacks, with three of these experts opening the phishing emails. This means that theoretical knowledge alone is insufficient for avoiding phishing attacks; instead, there is an urgent need for practical training for users, even if they have a technical background. This is so that they can be trained in how to recognize legitimate websites and emails. As a result of the current findings, the need for training to enhance users' security awareness appears to be of great importance.

VIII. CONCLUSION

In this paper, the effects of user awareness on the ability to detect phishing attacks were discussed and evaluated. Experiments were conducted on a sample of users in a real environment and the results were reported and interpreted. Significant positive effects were found, as regards the ability of users with high awareness to determine whether or not emails were legitimate, as opposed to being designed solely for the purpose of phishing. Moreover, 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; the aim being to evaluate the impact of modules dedicated to the topic of security, on the students' own security awareness.

REFERENCES

1. B. B. 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. FBI, "Annual Internet Crime Report 2017," 2017. [Online]. Available: https://www.fbi.gov/news/stories/2017-internet-crime-report-released-050718.
4. 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.
5. A. Alnajim, "A country based model towards phishing detection enhancement," *Int. J. Innov. Technol. Explor. Eng.*, vol. 5, no. 1, pp. 52–57, 2015.
6. 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.
7. "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.
8. IID, "eCrime Trends Report." [Online]. Available: http://internetidentity.com/resources.
9. L. F. Cranor, S. Egelman, J. I. Hong, and Y. Zhang, "Phinding Phish: An Evaluation of Anti-Phishing Toolbars," 2006.
10. 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.
11. S. Sheng, B. Magnien, A. Kumaraguru, Ponnurangam Acquisti, L. F. Cranor, and E. Hong, Jason and 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.
12. 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.
13. 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.
14. 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.
15. T. N. Jagatic, N. A. Johnson, M. Jakobsson, and F. Menczer, "Social phishing," *Commun. ACM*, vol. 50, no. 10, pp. 94–100, 2007.

AUTHOR PROFILE

Dr. Mohammed Alwanain is an information security and academic consultant. He is also a faculty in the Computer Science Department, at Majmaah University, Saudi Arabia. Dr. Alwanain obtained the BSc in Computer Science from King Saud University in 2004. He received the MSc in Software Engineering from Heriot-Watt University-Edinburgh in 2010 and the Ph.D. in Software Engineering from Birmingham University- United Kingdom in 2016. Currently, he is the dean of the Information Technology at Majmaah University. Dr. Alwanain's research interests involve network security, Internet security and frauds that encounter web applications especially online banking, e-commerce applications.

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)