THE IMPACT OF SECURITY AWARENESS ON USERS' SECURE BEHAVIOUR

Ibrahim Mohammed Alseadoon
College of Computer Science and Engineering, University of Hail, Kingdom of Saudi Arabia.
i.alsedon@uoh.ed.sa

(Paper presented at ICSC, 2019, KSA.

ABSTRACT: *Security awareness has been emphasized as an important solution for avoiding users' vulnerability in security. Moreover, users have been identified as the weakest link in the security chain. Our study investigates the impact of security awareness knowledge on users' secure behaviour. A quantitative method was used by the form of a questionnaire. The results show that users still the weakest link as they are not always performing secure behaviour despite their knowledge of risk. Furthermore, security awareness does not make a major difference in making users behave securely as shown by the results. Our study suggests that organizations should emphasis more on policies and regulations to make users behave more securely.*

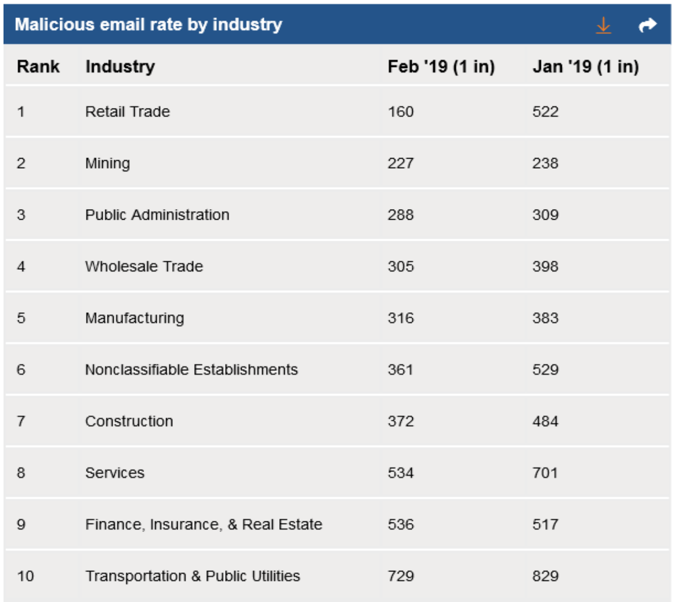
INTRODUCTION

Security attacks in recent years have been increased dramatically. Several solutions have been introduced to mitigate the problem of security attacks. Some of these solutions are mainly focusing on increasing users' awareness of security threats. Moreover, users are connected to the Internet and more information becomes available online. Devices are connected to the Internet most of the time and feed the Internet with various data which creates what we call big data. Big data are becoming more and more available on the Internet to provide services. Securing similar data becomes essential and necessary for making sure the continuity of Internet availability. Connected users and devises have the risk of losing privet data by unauthorized access or attacks. Various security measures have been introduced to secure such data from a breach. However, some of these measures have a high dependency on users who were identified as the weakest link the chain of security to protect data.

In the literature, there are several studies focuses on improving users' security by increasing their awareness about security attacks. These studies show that by improving users' awareness about security attacks, their security behaviour will increase which will result in protecting the data. Some of these studies focus on educating users about types of attacks by showing them attacking methods. Education has the vulnerability of making users vulnerable to unknown methods of attacks. For example, in security education, users were told not to click on unknown links in emails. However, one incident shows that one or two users had click on the similar link and compromised the organization security [1]. This incident shows the importance of preventing such links from reaching users, as attacks only need one user to compromise organization security.

Literature review

Security threats to Internet users have increased recently[2]. New threats are generated while known threats being tackled. Zero-day attacks have a high risk of making users becoming victims. Technical solutions cannot recognize zero-day attacks in order to prevent these attacks. Additionally, technical solutions cannot prevent all types of security threats. Unknown attacks success will depend solely on the users' decision. The problem is that users have been identified as the weakest link in the security chain. Therefore, solutions have been provided to increase users' protection by increasing users' security awareness. Improving security awareness has been introduced in various forms. The main discussed forms are education and security sins.



Malicious email rate by industry

Rank	Industry	Feb '19 (1 in)	Jan '19 (1 in)
1	Retail Trade	160	522
2	Mining	227	238
3	Public Administration	288	309
4	Wholesale Trade	305	398
5	Manufacturing	316	383
6	Nonclassifiable Establishments	361	529
7	Construction	372	484
8	Services	534	701
9	Finance, Insurance, & Real Estate	536	517
10	Transportation & Public Utilities	729	829

Figure 1: Malicius Email Data for the month of Jan- Feb 2019 [3]

Security education has been introduced to tackle the issues of Internet threats. One of these solutions is an online game which simulates a situation where users have to make a decision. Based on the users' decision, users will be informed if their decision was a correct and safe one. For example, Anti-Phishing Phil is an online game in which its main goal is preventing users from making security mistakes [4]. The results show that users who have been educated by the online game are significantly more able to identify threats. Furthermore, a study by Kumaraguru *et al*. shows that educating users about threats by exposing them to these threats is important [5]. Users who fall victim to attack are shown ways to prevent the attack. Their study has further shown a significant improvement in users' ability to protect themselves against attacks.

Security signs have been introduced to help users differentiate between a legitimate website and phishing websites [6-8]. The main goal of security signs studies is making users identify legitimate websites. For example, Internet Explorer has developed a green bar to show users that the visited website is identified and secure [9]. Website certificate is another way to say that the visited website has a known identified identity. Padlock icon has been introduced to web browsers to inform users that the visited website is encrypted and exchanged data are secured.

In summary, some studies have relied heavily on users' awareness to prevent threats. These studies show that increasing users' awareness has significantly changed their behaviour to make users behave more securely in the internet. Awareness materials are solely relying on educating users about certain attacks or behaviour. For example, there are four main behaviours which users have been told not to do: (1) users should not click on the suspected link in emails. (2) Users should not provide their password into an insecure webpage which does not show padlock icon. (3) Users should not connect to an open WiFi network. (4) Users should not use one password for various accounts. Our study tries to find if users with high-security awareness will stop making insecure behaviour.

Methodology

A quantitative method is used in our research to analyse the data. The used questionnaire was developed by Cisco Academy to test users' secure behaviour [10]. The questionnaire includes 8 questions where each question has its own mark. At the end of the questionnaire, participants were marked and given a number. High marks indicate insecure behaviour and low marks indicate more secure behaviour. The closest the mark to zero the more secure the user behave. Since our study targets Arabic users, we used the translated version of the questionnaire which was done by Osama [11]. Knowingly that each question in the questionnaire asks about certain behaviour.

Users' security awareness was measured to find its impact on users' secure behaviour. Participants were presented with one question about security awareness. The question used self-report with 3 points Likert scale [12]. The points were categorized as follows: low: 1, medium: 2 and high: 3. Additionally, Secure behaviour is divided into 4 main categories: high secure behaviour, secure behaviour, insecure behaviour and high insecure behaviour.

The questionnaire was uploaded into an online survey tool. A link was provided for the questionnaire, which was used for the distribution of the questionnaire. The link was sent to undergraduate students from both genders majored in computer studies. There was no incentive provided for participation to eliminate any de facto answers just for gaining the incentive. The questionnaire took around two weeks for data collection. Then, the questionnaire was no longer accepting answers from participants. Limiting answer period for two weeks only was to avoid any unwanted answers from participants who may send the link to their peers just for testing their secure behaviour. Therefore, we might get responses from participants outside our domain target.

RESULTS

The questionnaire was developed by security trainers to test users' secure behaviour. Therefore, the proposed notion is that these questions were developed by an expert. One issue faced these questions is that they were not tested for factor analysis. Our study implemented a factor analysis for these questions. The main theme for these questions was users' secure behaviour. Therefore, our study tested whether these questions (items) related to one construct. The result was less than the acceptable cut-off value [13]. Indicating each question (item) in the questionnaire represents a construct by itself.

The results from users' awareness indicate that users are average (Median is 2) and a little towards low (Skewness is 0.220). Additionally, participants were asked to report their victim situation (whether they have been victims). Only 13 percent reported that they have been victims where 62 percent of them were male. Furthermore, the questionnaire gives results from summing all the marks for each question to each participant. The overall results indicate that users' secure behaviour is low based on the sum of the results from participants marks (mean is 16).

The results indicate that participants are not always behaving securely. The percentage of each category for users' secure behaviour is 0,0,63, and 37 respectively. Notably, the results of the results came low in the first two categories is because of the distribution of the marks. High secure behaviour and secure behaviour are in the range between 0 and 3. Where insecure behaviour and high insecure behaviour range between 4 and 100. However, the results indicate that almost all users are in insecure behaviour marks. Users have done one or more insecure behaviour while using the internet.

The results indicate that there are three out of eight items show a significant impact on users' secure behaviour. The three items have a significant negative influence. These items are: using the same password for different accounts (Beta: -0.307, R square: 0.094, p=0.000), downloading and installing new software from the Internet (Beta: -0.250, R square: 0.063, p=0.001), and connecting to insecure WiFi (Beta: -0.265, R square: 0.070, p=0.001).The rest of the measured items do not show any significant impact. The results indicate that high awareness will make users less reluctant to use the same password for different accounts, downloading and installing unknown software and connecting to insecure WiFi.

DISCUSSION

The results obtained in our study show that users' awareness has a significant impact on some of the users' secure behaviour. However, the impact of awareness is very limited. This indicates that users' awareness is not the main factor that forces users to behave securely. As we observed in our results that the R square is less than 0.1, which indicates low impact. For example, this study shows that users choose to use the same password for different accounts. This behaviour indicates low securely behaviour. Security experts always advise users to choose different passwords for different accounts. The reason behind this advice is that if one of these accounts was preached other accounts will remain secure (protected) since they have different passwords.

Behaving less securely does not always mean that users are not afraid to lose their accounts. The reason can be that users choose to have one password for different accounts as it is easy to remember. Various passwords are hard to remember as users' memory tends to forget. Additionally, our study did not measure password strength. Users may use a strong password in different accounts believing that these accounts will be secured. However, attackers may benefit from this behaviour by obtaining a list of passwords associated with accounts names. Then, whenever these account names were identified there is a list of passwords to be tried.

Our study suggests that there is a need for another factor supporting users'' security awareness which can be organizations policies. Policies can mitigate this vulnerability by forcing users to choose different passwords. However, there is one issue which is that service providers cannot know whether these passwords were used in other places. One possible way is creating a list of known passwords and easy passwords to prevent users from choosing such passwords.

Several studies suggested that informing users about security practices will improve their ability to detect attacks. For example, Anti-Phishing Phil is an online game that educates users about phishing emails ways and how users can protect themselves from it [4]. The education game had prevented users from clicking on the suspected link. However, some insecure behaviour does not always prevent users from performing the behaviour. For example, connecting to insecure (open) WiFi is considered as risky behaviour. An attacker may exist in the network and performance monitoring and listening to traffic. Therefore, if a user needed an Internet connection and the available network is a less secure network. S/He may take the risk of connecting to an insecure network, as it is the available way to complete an urgent task. It is suggested that users will be more willing to take the risk if the loss is not certain [14]. Policies can be applied to enforce users not to connect to open WiFi networks if it involves transferring sensitive information.

The results indicate that the majority of users are behaving less securely while surfing the Internet. One of the reasons for the conclusion of the results is, that following all security devices while surfing the Internet, is hard. There are times where users need to connect to the Internet and the available network is insecure. Choosing different passwords for each account is hard to remember.

The battle between security and usability is always facing users. Users may choose to take the risk if the gain is bigger than the risk. As previously mentioned, users may choose to take the risk of connecting to an open WiFi connection for the big gain of completing the task in hand. Users who become victims have shown risk-taking behaviour [14]. In order to reverse risk-taking behaviour, there is a need to make users lose for behaving insecure behaviour which can be achieved by organizations policies. Our study suggests that users' security awareness by itself is not enough to guarantee secure behaviour. Security awareness needs to be accompanied by policies to increase users' secure behaviour.

CONCLUSION

Awareness insecurity has been provided to be one of the significant factors to prevent insecure behaviour conducted by users. The results obtained by our study indicate that the impact of security awareness on users' secure behaviour is limited. Our study conducted a questionnaire on users and the results show that users will behave insecurely when policies allow them. For example, users may choose one password for different accounts since these accounts cannot know if the provided password has been used elsewhere. In order to emphasize security on users and increase their security behaviour, organizations need to implement new policies in addition to security awareness to prevent users from behaving insecurely.

REFERENCES

1. Choney, S. *New York Times hacked, Syrian Electronic Army suspected - NBC News* <https://www.nbcnews.com/technolog/new-york-times-hacked-syrian-electronic-army-suspected-8C11016739>. 2013 [cited 2015 12-9].
2. Ahamad, M., et al., *Emerging cyber threats report for 2009.* Georgia Institute of Technology, 2008.
3. Corporation, S. *Monthly Threat Report | Symantec* <https://www.symantec.com/security-center/publications/monthlythreatreport>. 2019 [cited 2019 1-4].
4. Sheng, S., et al. *Anti-phishing phil: the design and evaluation of a game that teaches people not to fall for phish*. in *Proceedings of the 3rd symposium on Usable privacy and security*. 2007. ACM.
5. Kumaraguru, P., et al. *Getting users to pay attention to anti-phishing education: evaluation of retention and transfer*. in *Proceedings of the anti-phishing working groups 2nd annual eCrime researchers summit*. 2007. ACM.
6. Aburrous, M. and A. Khelifi. *Phishing detection plug-in toolbar using intelligent Fuzzy-classification mining techniques*. in *The international conference on soft computing and software engineering [SCSE'13], San Francisco State University, San Francisco, California, USA*. 2013.
7. Chou, N., et al., *Client-side defense against web-based identity theft*, in *In Proceeding of the 11th Annual Network and Distributed System Security Symposium (NDSS '04)*. 2004.
8. Herzberg, A. and A. Gbara *Protecting (even) Naive Web Users, or: preventing spoofing and establishing credentials of web sites*. 2004. 1-26.
9. Blakemore, E. *Internet Explorer goes green for "go" - Microsoft Security* <https://www.microsoft.com/security/blog/2008/12/09/internet-explorer-goes-green-for-go/>. 2008 [cited 2018 12-5].
10. Academy, C.N. *Get Started Today In Introduction to Cybersecurity | Networking Academy* <https://www.netacad.com/ar/courses/security/introduction-cybersecurity>. 2018 [cited 2018 12/12].
11. PDF, F. مقدمة في الأمن السيبراني *par Osama Mohammed Moustaf Hosam Elde - Fichier PDF* <https://www.fichier-pdf.fr/2017/11/14/fichier-pdf-sans-nom-1/>. 2018 [cited 2018 4/12].
12. Likert, R., *A technique for the measurement of attitudes.* Archives of psychology, 1932.
13. Hair, J., et al., *Multivariate data analysis–a global perspective (global edition).* Edinburgh gate, 2010. **07**.
14. Alseadoon, I.M., et al., *Typology of phishing email victims based on their behavioural response.* 2013.