User Response When Faced With Cyber Threats

[Yaw Owusu], [Tedros Beyan]

ABSTRACT

There are many cyber attacks that occur daily. These attacks against machines and users can occur due to the actions of users. What motivates users to fall victim to cyber attacks is what is investigated in this paper. Motivations such as emotion, opportunity and past behaviour are evaluated. We conducted a 26 participant study in which the three motivations were embedded in various vignette questions along with three common cyber attacks. These three cyber attacks were phishing, clickjacking and trojan horse. The results of the study showed that users were motivated by emotions and past behaviour. The results also showed that users who were trained and given vignettes with multiple cyber attacks performed almost the same as users who were untrained and were given single attack vignettes.

Delivered: May 3rd 2020

Introduction

Staying safe while using the internet is becoming increasingly difficult due amount of cyber attacks. While some users may think that they are cannot be victims of cyber attacks because they are not as attractive of a target as large organizations, attacks against users have become commonplace. There have been many attempts to educate users about cyber attacks such as phishing training and cyber threat awareness training [7]. However, there are still cyber attacks against users that are untrained and even those that are trained. This might be due to the fact as people become more educated, hackers also become more sophisticated. However the attacks which hackers or cyber attackers use have always had the same base formula.

- The base idea of trojan horse is to trick users into downloading software that seems to be real but has hidden malicious intent.
- The base idea of clickjacking is to trick users into clicking hidden buttons or overlays which the user did not intend.
- The base idea of phishing is to trick the user into thinking a fake entity or person is real.

If these tricks have always been the same, then why do even trained users still fall victims to these attacks[7]. The reason why victims fall for these tricks is what this investigation tries to explore. We also try to understand how users react to singular and multiple cyber attacks. In this investigation we ask if:

1. Will participants be able to identify a cyber threat even after they have been informed about the nature of the threat?
2. How do different variables such as emotions, past behaviour and getting an advantage or opportunity affect participants reactions to threats?
3. When two or more cyber security are presented to the participants will participants be able to identify both threats?

In our investigation we use try to understand how reasons such as emotion, opportunity and past behaviour influence trained and untrained participants to become victims of cyber attacks such as clickjacking, Trojan horse and phishing. We use vignette type survey to understand these user reactions. We create various scenarios based on these reasons which are also embeded with various cyber attacks. In our investigation, we make the following hypotheses:

1. Participants that are trained and given easy questions will be able to identify or recall the meaning of each cyber security threat
2. Participants that are <u>not</u> trained and given easy questions will not perform better, than those that were trained and given easy questions, if they are asked to identify or recall the meaning of each cyber security threat
3. Participants that are trained and given complex questions will perform worse than those given easy question if they are asked to identify or recall the meaning of each cyber security threat
4. Participants that are <u>not</u> trained and given complex questions will perform the worst if they are asked to identify or recall the meaning of each cyber security threat
5. Participants who are trained about the three cyber threats before answering questions will do better than those who are untrained in both one threat and two threat questions.
6. Participants will be susceptible to cyber threats motivated by opportunity than those which are emotional or of past behaviour

Related Studies

The goal of our experiment is to understand the reasons why users become victim to cyber attacks and also to investigate user retention of cybersecurity training. The reason why cyber security training is important is because users are the most known causes of cyber attacks. Ross et al. found that almost 90% of cyber attacks were caused by human error or behaviour [3]. That is why security awareness is very important. Jemal et al. conducted a study on various types of security awareness teaching methods with game, text and video teaching methods [4]. They found that text based teaching methods did not have as much retention when compared to video and game teaching methods. However their method of text based teaching only shows two types of phishing which are email phishing and URL phishing. Our investigation looks at not only phishing, but other types of cyber threats which the participants of our investigation have to identify. In our investigation we use some of their ideas and examples of both types of phishing to craft the questions.

It is important that users are able to understand and answer these questions because not many users are aware of these types of attacks. A study by Consolvo et al. found that non-expert users were unaware of the strategies used to protect themselves against cyber security threats [2]. Their work only encapsulates protection rather than detection of cyber security threats unlike our investigation. The work of Consolvo et al. does highlight mental models of certain threats which was used to craft questions which identify metal models users have that are not beneficial. For example in their study many of the non-expert participants state that they used anti-virus software against malware. However anti-virus malware might not protect these participants from clickjacking which is a web-based cyber attack.

Even though some users are educated on cyber security threats, not all of them fully understand how to detect these threats. In a study by Wash et al. they found that many users understand security threats in the abstract sense but may not believe they themselves are at risk which is a big misconception among users [1]. However what this work shows is that if users do not believe that they are at risk then then they might not be able to tell if they are under real attack. This is the difference between Wash et al. investigation and our paper. Our paper tests whether users are able to identify cyber attacks in many different scenarios. The scenarios in this paper are based on some of the mental models presented by Wash et al.

Phishing

Phishing is a common cyber attack that many users who do not have enough education about cyber security become victims of. This was the case in an investigation by Dhamija et al. who found in their investigation that many users were not able to distinguish phishing websites and authentic ones [7]. The examples in the Dhamija et al study are used to create a combination of phishing and other cyberattacks. The difference between this study and the Dhamija et al study is that the participants were shown actual websites that were designed for the study. There have been studies that basically just educates users rather than test and an example of such a study was conducted by Chaudhry et al. In their study they did not test participants unlike our study [5]. However the study by Chaudhry et al highlights many attributes of phishing which are used in our investigation. Another study which shows many user attributes concerning phishing was conducted by Marforio et al. In their study, they used software to monitor user behaviour on smart phones and detect potential phishing attacks. The user behaviour in this experiment are also used to help formulate parts of our study. However in our study the participants had to detect the phishing for themselves.

Smartphones like all other phones can be a medium for phone phishing attack. A study by Tu et al found that many of the participants in their study were tricked by phone call Id's that were similar to authentic Id's [6]. In fact 60% of the participants that received fraudulent calls from a phone ID of the "W-2 Administration" believed the call to be authentic although such organization did not exist. The different phishing ID's used in this experiment are used in our experiment however the difference is that our experiment does not involve actual phone calls but rather text based scenarios of cyber attacks. Scenario based training are very common in cyber security training. In two different studies by Arachchilage et al and Wen et al, game based phishing scenarios were used to test participants about their phishing detection abilities [8,11]. Some of these scenarios are used in this paper however the video game aspect of both Arachchilage et al and Wen et al could not be used in this study.

There have been studies on phishing in real life environments such as the work place. An example of such a study was conducted by Ho et al in which they investigated lateral phishing within companies unlike our investigation [9]. The Ho et al investigation highlights phishing through trust which is an attribute that is used in our investigation.

Clickjacking

Clickjacking is another user initiated cyberattack. Clickjacking occurs when a user clicks on an item on a web page for an intended purpose however the item that was clicked has other intentions which are not known to the user and are often malicious. There have been many studies on how easy it is for users to fall victim to clickjacking. Hazhirpasand et al. were able to trick 95% of its participants with clickjacking and Akhawe et al were able to trick over 90% of its participants with clickjacking [12,13]. These studies do not teach participants about clickjacking unlike our study which teaches participants before testing them. However both studies give great insights on how users can be tricked, all of which are used in our experiment. User's inability to identify clickjacking is not the only problem. Another problem is that many popular websites are vulnerable to clickjacking attacks placed by hackers. A study by Kim et al. found that 78% of popular websites around the world are vulnerable to clickjacking attacks [15]. The forms of clickingjack used in their experiment was used in this experiment and the participants in our experiment were tested on those forms unlike the investigation by Kim et al.

Although the papers discussed above show how easy it is for users to fall victim to clickjacking, there have been many studies that try to show how to detect clickjacking. One of such studies was conducted by Jyotiyana et al which shows various ways in which clickjacking is embedded in websites and how they can be detected [16]. The techniques used in this study is used in our experiment to formulate questions about clickjacking. Websites are not the only things that have been studied about clickjacking. There have also been studies that show user behaviour before being clickjacked. Faghani et al. studied user interaction on social media and identified behaviours that lead to clickjacking [14]. These behaviours are attributes that are also used to formulate questions about clickjacking in our experiment.

Trojan Horse

Another form of cyber attack which is difficult to detect is a malware download or Trojan horse attack. A study by Baychev et al. showed how spearphishing is used to influence users to download malware which is very similar to our investigation which also uses both combinations of cyber attacks [17]. The difference is that the order in our investigation is different. In their investigation the users are spearphished into downloading malware but in our investigation the malware download can cause a user to be spearphished.

There can be other behaviours which motivates users to download malware. Two studies have shown insights into such behaviours. In the first investigation, Levesque et al. monitor user behaviour and try to predict future probability of malware download [18]. The second investigation by Canali et al. looks at various models that affect user behaviour of malware download [19]. Both of these studies give insights to user motivation for the download of malware, which is used to set up the question about malware download.

Methodology

Group Set Up

In this study there were be 4 groups who were be divided by their training and amount of cyber threats(Table 1).

Table 1. Participant Groups

	. Trained .	. Not-Trained .
One Threat	Trained + One Threat	Not-Trained + One Threat
Two Threat	Trained + Two Threat	Not-Trained + Two Threat

- **Trained + One threat** This group was given the definitions of the three cyber threats before the experiment. These participants were then tested on these definitions to evaluate their retention. After the testing the participants proceeded to answer vignette questions, each consisting of a single cyber threat.
- **Not-trained + One threat** This group was not given the definitions of the three cyber threats before answering the vignette questions. However the participants in this group were given vignette questions which consisted of a single threat
- **Trained + Two threat** This group was given the definitions of the three cyber threats before the experiment. These participants were then tested on these definitions to evaluate their retention. After the testing the participants proceeded to answer vignette questions, each consisting of a two cyber threat.
- **Not-trained + Two threat** This group was not given the definitions of the three cyber threats before answering the vignette questions. However the participants in this group were given vignette questions which consisted of a two threat

Vignette Format

Participants in the 4 groups were each given 9 vignettes questions. For each participant, the 9 vignettes consisted of 3 reason themes. These themes were emotional, opportunity and past behaviour. Each theme had 3 vignette questions which totalled the 9 vignettes. Each themed reason had one or combination of two cyber threats depending on the group the participant was in(Fig. 1).

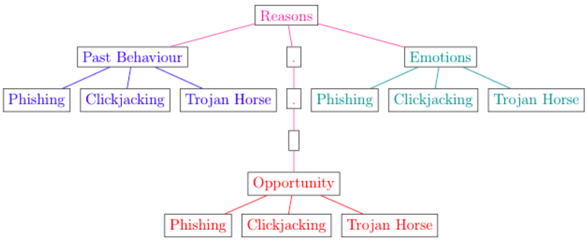

Figure 1. Vignette combinations

Recruitment

The platform which the survey was administered was Google Forms. The participants were recruited through word of mouth. In order to avoid multiple submissions by one participant, Google Forms required each user to login with their Gmail account once. The order of each question was randomised. The choices for each vignette question was also randomised.

Data Analysis

The significance of the data was calculated using the R program [20]. This program was used to calculate the significance between all the groups.

Table 2. Demographics

Demographic	Category	Number of Participants
Gender	Male	12
	Female	14
Age	18-20	3
	21-24	8
	25-36	15
Education	High School	3
	College	16
	Masters	5
	PhD	2
Race	Asian	3
	African American	19
	Caucasian	5
Employment	Full Time	9
	Military/Army	2
	Part Time	13
	Unemployed	1

Results

In this section, we detail the findings of our study. We start by presenting the demographics of our participants, and then discuss the key findings from our study organised according to the research questions.

Participants

In this study we had a total of 26 participants. The only demographic that showed balance was gender. All the other demographics were skewed(Table 2.). There was also an imbalance between the participants in the 4 groups. The last group, Not-trained + Two threat, had 5 participants while the other groups had 7(Table 3).

Table 3. Participant Groups

	. Trained .	. Not-Trained .
One Threat	Trained 7 One Threat	Not-Trained 7 One Threat
Two Threat	Trained 7 Two Threat	Not-Trained 5 Two Threat

Cyber Threat Training

The partipants in the in trained groups were given simple questions about the three cyber threats which they were given the definition of. Majority of the participants were able to answer the questions about clickjacking and trojan horse correctly. However many of the participants got the question on phishing partially correct.

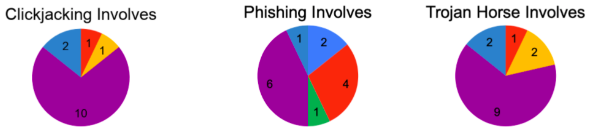

Figure 2. Correct = Purple, Partially Correct = Yellow, Red, Blue

One Threat Groups

The result of the participants in the one threat group showed significant differences between the untrained participants and the trained participants. The untrained participants were susceptible to more cyber attacks than trained group. Both groups have were victims of cyber threats when the theme was either emotional or past behaviour.

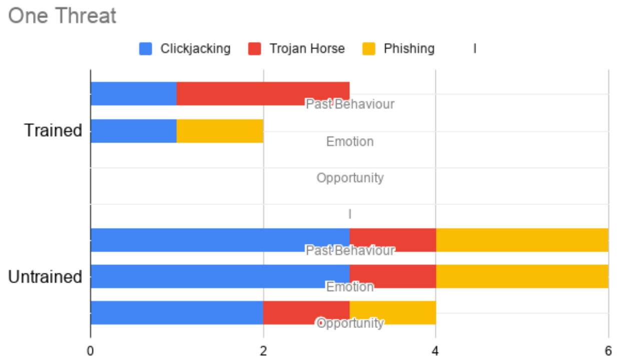

Figure 3. One

Two Threat Groups

The result of the participants in the two threat group showed significant did not show much difference due to the unequal number of participants. However, participants in the trained two threat group performed almost as bad as the participants who were untrained in the one threat group(Fig 4).

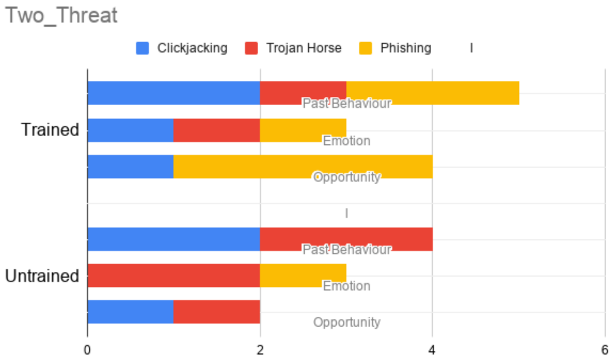

Figure 4. Two Threat Group

Discussion

Training

The participants in the trained groups performed well on their training. However almost half of the participants answered the phishing question correctly. The phishing training required the participants to select the option which encompasses all the components of a phishing attack. However a good fraction of the participants chose a partial definition of the phishing attack. This might be due to the fact that may be the component of phishing which they are most familiar with.

Reason for Attack

Participants fell victims to cyber attacks that were centered around the theme of emotion and past behaviour. This rejects the hypotheses that participants were more likely to be susceptible to reasons based on opportunity. This might be due to the fact that opportunities presented in the vignettes were not very relevant to participants.

Cyber Threats

Hypothesis 1-4 rejected the null hypothesis as seen in the data. However, hypothesis 5 is rejected because participants that were trained and given two threat vignettes performed almost as bad as participants in who were untrained and given one threat vignettes. Participants were more susceptible to clickjacking and phishing than they were to Trojan horse attacks.

Limitation

In this study the number of participants were not enough calculate significance between the groups. Also there little diversity in demographics in terms of race, education and age. Another limitation in this investigation is the vignettes that were developed. These vignettes may have not been as influential to the participants.

Conclusion

Data shows some significance when comparing One vs Two threat situations in both reasons and type of attack. This finding might need further investigation into why participants who were trained in two threat cyber threat situations performed almost as bad as those who were not trained and given one threat cyber threat situations. Reasons based on past behaviour made participants more likely to fall for cyber attacks. This shows that needs cyber security training needs emphasize on past behaviour when training users.

Acknowledgements

We would like to take this opportunity to thank Dr. Khan for making this investigation possible.

References

[1] Rick Wash. *Folk models of home computer security.* In Proc. SOUPS '10, page 1, New York, New York, USA, 2010. ACM Press.

[2] Iulia Ion, Rob Reeder, and Sunny Consolvo. "*...no one can hack my mind": Comparing Expert and Non-Expert Security Practices.* In Symposium on Usable Privacy and Security (SOUPS), pages 327{346, jan 2015.

[3] Kelly, Ross, et al. *Almost 90% of Cyber Attacks Are Caused by Human Error or Behavior.*" ChiefExecutive.net, 7 May 2017, chiefexecutive.net/almost-90-cyber-attacks-caused-human-error-behavior/

[4] Abawajy, Jemal. "*User preference of cyber security awareness delivery methods.*" Behaviour Information Technology 33.3 (2014): 237-248.

[5] Chaudhry, Junaid Ahsenali, Shafique Ahmad Chaudhry, and Robert G. Rittenhouse. "*Phishing attacks and defenses.*" International Journal of Security and Its Applications 10.1 (2016): 247-256.

[6] Tu, Huahong, et al. "*Users really do answer telephone scams.*" 28th USENIX Security Symposium (USENIX Security 19). 2019.

[7] Rachna Dhamija, J D Tygar, and Marti Hearst. *Why phishing works.* In Proc. CHI '06, number April, pages 581{590, New York, New York, USA, 2006. ACM Press.

[8] Arachchilage, Nalin Asanka Gamagedara, Steve Love, and Konstantin Beznosov. "*Phishing threat avoidance behaviour: An empirical investigation.*" Computers in Human Behavior 60 (2016): 185-197.

[9] Ho, Grant, et al. "*Detecting and characterizing lateral phishing at scale.*" 28th USENIX SecuritySymposium (USENIX Security 19). 2019.

[10] Marforio, Claudio, et al. "*Evaluation of personalized security indicators as an anti-phishing mechanismfor smartphone applications.*" Proceedings of the 2016 CHI Conference on Human Factors in ComputingSystems. 2016.

[11] Wen, Zikai Alex, et al. "*What. hack: engaging anti-phishing training through a role-playing phishing simulation game.*" Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems. 2019

[12] Hazhirpasand, Mohammadreza, Mohammad Ghafari, and Oscar Nierstrasz. "*Tricking Johnny into Granting Web Permissions.*" arXiv preprint arXiv:2002.08463 (2020).

[13] Akhawe, Devdatta, et al. "*Clickjacking Revisited: A Perceptual View of UI Security.*" 8th USENIX Workshop on Offensive Technologies (WOOT 14). 2014.

[14] Faghani, Mohammad R., and Uyen T. Nguyen. "*A study of clickjacking worm propagation in online social networks.*" Proceedings of the 2014 IEEE 15th International Conference on Information Reuse and Integration (IEEE IRI 2014). IEEE, 2014.

[15] Kim, Daehyun, and Hyoungshick Kim. "*Performing clickjacking attacks in the wild: 99% are still vulnerable!.*" 2015 1st International Conference on Software Security and Assurance (ICSSA). IEEE, 2015.

[16] Jyotiyana, Priya, and Saurabh Maheshwari. "*Techniques to Detect Clickjacking Vulnerability in Web Pages.*" Optical and Wireless Technologies. Springer, Singapore, 2018. 615-624.

[17] Baychev, Yanko, and Leyla Bilge. "*Spearphishing malware: Do we really know the unknown?.*" Inter-national Conference on Detection of Intrusions and Malware, and Vulnerability Assessment. Springer,Cham, 2018.

[18] Levesque, Fanny Lalonde, Jose M. Fernandez, and Anil Somayaji. "*Risk prediction of malware victimization based on user behavior.*" 2014 9th International Conference on Malicious and Unwanted Software: The Americas (MALWARE). IEEE, 2014.

[19] Canali, Davide, Leyla Bilge, and Davide Balzarotti. "*On the effectiveness of risk prediction based on users browsing behavior.*" Proceedings of the 9th ACM symposium on Information, computer and communications security. 2014.

[20]RStudio Team (2018). RStudio: Integrated Devel-opment for R. RStudio, Inc., Boston, MA URL http://www.rstudio.com/.