AN EXPERIMENT: PHISHING ATTACKS IN THE WORKPLACE

***VALBONA DHJAKU[1], IGLI TAFA[2], DORINA UKA[2], KETRINA BICI[2]**

[1]Credins Bank, Information Technology Department, Tirana, Albania

[2]Polytechnic University of Tirana, Department of Computer Engineering, Tirana, Albania

e-mail: vdhjaku@gmail.com

Abstract

An observational study was conducted in a telecommunication company, where 20 participants were recruited and were exposed to social engineering in the form of a phishing email over the course of a week. This email attack attempted to get personal information on the employees of the company and entice them to click on the link included on the email. The aim of the study is to determine the risks or the phishing cyberattack in the workplace by observing employee's responses. The participants of the study were divided in two different groups. The first 10 participants had an increased awareness of cyberattacks as they were primed to be cautious about the possible phishing emails that they could be exposed to. The second group received no instructions on how to deal with such attacks and had a lower level of awareness regarding cybersecurity. The study explored the influence of different factors such as: gender, level of awareness and perceived importance of security.

Key words: Phishing, email attack, security, cyber risk.

Përmbledhje

Një studim u krye në një kompani telekomunikacioni, ku 20 prej pjesëmarrësve u rekrutuan dhe j'u ekspozuan 'inxhinierisë sociale' në një formë të phishing nëpërmjet postës elektronike një here në javë. Ky sulm me email u përpoq të merrte informacione personale mbi punonjësit e kompanisë dhe t'i nxiste ata të klikonin në linkun e përfshirë në përmbajtjen e-email. Qëllimi i studimit është të përcaktojë rreziqet ose sulmin kibernetik phishing në vendin e punës duke vëzhguar përgjigjet e punonjësve. Pjesëmarrësit e studimit u ndanë në dy grupe të ndryshme. 10 pjesëmarrësit e parë kishin një sensibilizim të shtuar ndaj sulmeve kibernetike, pasi ishin të përgatitur për të qenë të kujdesshëm në lidhje me e-mail-et e mundshme phishing që mund të ekspozoheshin. Grupi i dytë nuk mori udhëzime se si të sillen me sulme të tilla dhe kishin një nivel më të ulët të ndërgjegjësimit në lidhje me sigurinë kibernetike. Ky studim vlerësoi ndikimin e faktorëve të ndryshëm si: gjinia, niveli i ndërgjegjësimit dhe rëndësia e perceptuar e sigurisë.

Fjalëkyçe: Postë elektronike, siguri, sulm kibernetik.

Introduction

The human error is considered by many scholars the weakest link when it

comes in cybersecurity. The increased usage of internet in the workplace has resulted in an increased exposure to the cybersecurity attacks and the exploitation of the human factor. (Mayhorn, *et al.* 2015). When cybercriminals use phishing methods in order to steal information and deploy malware they target the judgment of the employee rather than the technical security measures taken by the company. (Gratian, *et al.* 2018).

A very common method of exploitation is the usage of spam email. Spam involves advertising through emails, SMS texts, social network messages but they can also include viruses regardless of the medium used to send the message to the recipient. A world-wide average daily volume of spam was 422 billion just in January 2018 and it makes for 85 percent of all emails sent (Talos, 2018).

Phishing emails are some of the most effective and well-known cyberattacks. They lead to millions of compromised credentials and they make for 90 percent of the total data breaches (Retruster.com 2019). Phishing scams are not only consisting of emails. Some other popular phishing scam methods include but are not limited to spoofed websites and fake phone calls. According to scholars, anyone can fall victim of phishing attacks regardless of technical background. The impacts of these attacks can have profound consequences that cause a lot of financial harm to the company and can be detrimental to the business continuity.

The threat of phishing emails poses widespread economic and social consequences. However, the susceptibility to spam emails depends on a lot of factors and is not universal. Variables like age, gender and technical experience have an effect on how successful the phishing attack is going to be. (Gavett *et al.* 2017). This study aims to explore the susceptibility and the victimization of the employees in the workplace and provide insight on the effectiveness of raising awareness on cybersecurity threats. To accomplish this, 20 employees of a telecommunication company were recruited. They were divided in two different groups. The first group was given information on phishing emails and the other was not provided with such information. Then, the employees were exposed to fake emails designed and sent by the researchers. They're actions and interaction with the phishing emails were then observed and categorized. Phishing is one of the most effective and well-known cyber threats, leading to millions of compromised credentials and contributing.

Related Works and theoretical explanation

There are many definitions of 'spam', but in general if can be said that it includes all unsolicited electronic messages that are usually, not necessarily, sent in bulk transmission. Many technologies are used and combined with social techniques in order to lure and get information from the victim, through

inciting a response by email. The purposes of phishing ranges from delivering malware or ransomware to obtaining information for the usage of identity theft.

The three elements comprising a typical phishing attack, suggested by (Chaudhry *et al.* 2016), are:

- a lure,
- a hook,
- a catch.

The lure involves from who the email is being sent from, in most cases it looks like it is being sent from a legitimate person or organization and it is strengthened by the exploitation of curiosity, fear and empathy.

Other exploitative factor can be involved to further make the phishing attack more effective such as:

- greed (e.g., winning a lottery contest),
- lust or vanity (e.g., writing from someone coming from an adoration point of view or offering a dream job position).

A thorough list of factors that either facilitate or hinder the success of a phishing attack can be found by De Kimpe, *et.al* 2018). After the victims are convinced that the email is authentic, then you need to incite a response divulging sensitive information. Various techniques involve:

- sending the email for a likable source;
- implicate reciprocity (e.g., returning favors);
- social legitimacy (e.g., a large amount of people are already participating);
- creating a sense of urgency or scarcity (e.g., this sale is going to end after a few days or hours).

These techniques will help you increase the likelihood.

In some cases personalized data is used in the lures, so that they become a subcategory of phishing, 'spear phishing'. Spear phishing is contextual, with emails containing specific information is familiar or important to the victim (De Kempe, Walrave, *et.al* & Ponnet, 2018). To obtain such relevant information to make the technique possible, the attacker spends a considerable amount of time obtaining it, and then creates the personalized email for every victim (Caputo Pfleeger, Freeman, & Johnson, 2016). These emails have the tendency to impersonate companies that are well known, relationships that are trusted or

contexts that have personal relevance to the individual (De Kempe *et al.*, 2018).

If a phishing or spear phishing email succeeds, it all depends on how well it is crafted to deceive the respective victim. This study further tests the existing literature that focuses on the structures of phishing emails (e.g., use of pictures, incorrect of misspelled attachment files; (Parsons, *et al.* 2017). Targets have shown to be prone to fall victim to phishing emails if these contain personalized information relevant to them (Benenson, *et al.* 2016).

The effect of various social engineering strategies have been tested by (Butavicius, *et al.* 2017), by sending a mixed emails to 117 university students. Some were genuine, some phishing and spear phishing emails. The finals results indicated that students were hesitant to classify as fraudulent and were worse at recognizing spear phishing attempts over generic phishing attempts. It was also found that if the email was sent from someone who held power over the students, they were more likely to fall victim to them.

Some general insight is offered from the survey by the Australian Institute of Criminology (AIC) in 2017, where they concluded that individuals are more cautious or careful as they navigate dangerous environments, once they have been notified or aware of their respective risk. After a rise in the percentage of identity theft in the past 12 months, the general public took various security measures such as changing passwords, signatures and voice recognition.

The suggestion that experience and technical knowledge increases the levels of security measures individuals take, has been seen in (Sun *et al.*, 2016). Though the impacts that this expertise has on phishing attempts is still not fully understood. (Luga *et al.* 2016), in their role- play experiment tested the relationship between user 'usage' and phishing detection by asking participants to distinguish genuine web pages in comparison to phishing pages. The result was that people with more 'experience' were harder to fool.

The study conducted by Abassi and colleagues' (2016), tried to question the assumption that people who feel unsafe are more likely to be vigilant and deployed countermeasures, meaning they were not necessarily more vulnerable. But the results were that people who were aware of phishing, spent a lot of time online, knew the difference between a phishing page and a genuine one and also had been phished in the past, were the best at detecting phishing. But at the same time some of these traits, showed negative influence because of overconfidence. But generally the more people were aware of Internet risk and common vulnerabilities, the more they were capable of avoiding phishing attempts.

Experimental environment

This experiment seeks to explore the behavior of employees in the workplace

regarding phishing attacks. We achieve this by conducting an observational study in a telecommunication company. The participants were selected randomly and we have tried to form a diverse group consisting of different age groups, gender and different awareness levels of cyberattacks. Firstly, 20 participants were selected and divided in two separate groups. The first group was provided with general information on the importance of cybersecurity and they were specifically informed about phishing attacks. The second group did not have the afore mentioned information. This division helped us differentiate the employees that had some basic level of awareness and likewise the ones that lacked the latter.

The retrieval of data was made possible by the company with the consensus of the employees participating in this study. Data such as age, gender, work experience, emails, awareness level towards cybercrime were provided in the early stage of communication with company's representatives.

To accomplish the goal, a simulated phishing email was sent out to employees and their interactions were observed. The observation was conducted over a period of one week, during which email content was sent to them. As mentioned previously participants were also compared across two conditions: employees with phishing attack awareness condition, and others that received no such information.

Characteristic	Participant (number=20)
Gender	%
Male	50%
Female	50%
Age	
22-25	40%
Over 25	60%

Table 1. Data Description

We managed to create and send the phishing email, and also recorded data about the interaction participants had with the fake phishing email. A never-ending loading page hosted our participants if deceived by the fake phishing email. The emails were crafted to appear to have been sent by a (fake) person or organization. Access to an open SMTP server is required in order to distribute these emails. The script would connect to the SMTP server and send the email data, including the sender's email address. Email clients, such as Hotmail,

Gmail, and Outlook, include the sender's email address in the emails that they send, however the SMTP standard does not require the correct originating email address, permitting us to send emails that appear to have originated from other people or organizations.

Three different types of responses were recorded:

- No response. The email never got to target's inbox
- Received but ignored. The participant opened the email but took no action. This may or may not be because they identified the email as fraudulent.
- Received and responded. The participant takes action in response. This could be sending an email in reply, clicking on a link within the email.

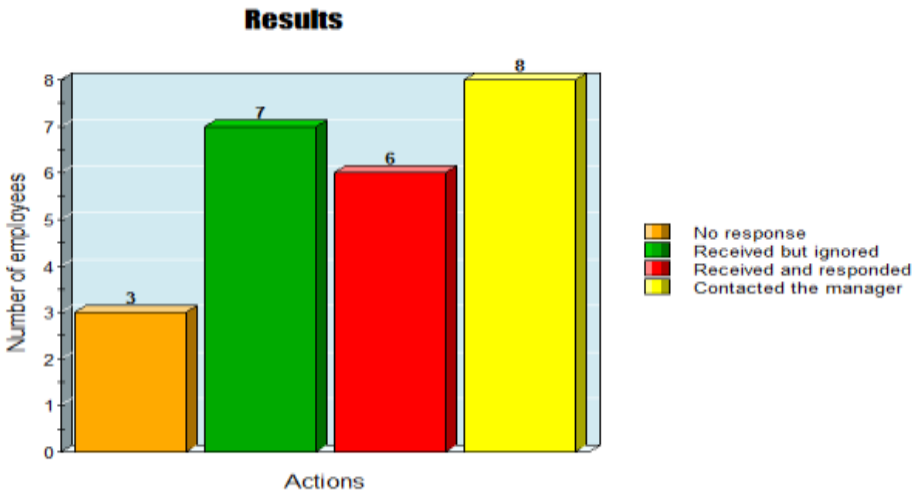

Image 1. Experiment results

From the data gathered in the end of the experiment, taking a group of 20 employees there was observed that 3 of them gave no response at all, 7 of them received the email but ignored it, 6 of the participants received the email and responded and 8 of them contacted the manager. As shown above, the total number of actions is greater than 20.

This is explained by the fact that 4 of the actions overlapped since 3 of the participants that received and ignored also contacted their managers and one of the participants that responded became suspicious after they received the email and
responded.

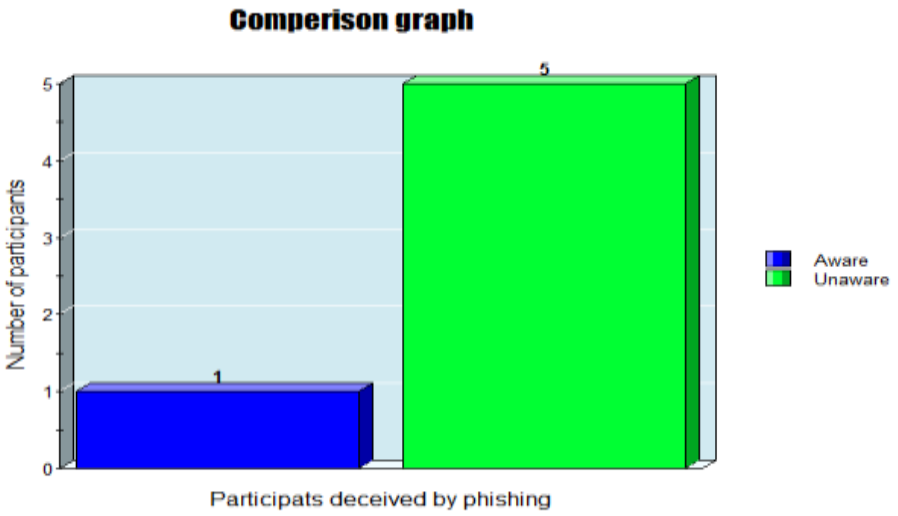

Image 2. Comparison graph

The total number of the participants deceived by the email was 6 and 5 of them were not previously made aware of the risks that cyberattacks and phishing scams pose. Regardless of being aware, one of the participants was deceived by the phishing email.

Interpretation

In the previous chapter we briefly covered the results of the experiment conducted. In this chapter we are going to provide an explanation and further interpret the data gathered based on the behavior and the actions of the participants.

As expected, the participants that were less aware of cyberattacks and phishing emails were more susceptible to being victims of such attacks. Out of the 6 participants that were deceived by the phishing email the majority, specifically 5 of them were the ones that were not given information on cybercrime. This shows that the level of awareness has a positive influence on protection from social engineering.

Furthermore, based on the working experience of the employees, we observed that the participants that fell victims of the attack had less working experience. 3 out of the 5 participants that were deceived had less than 1 year of working experience. They lacked sufficient training and as claimed by the managers they had no previous knowledge on cybercrime. Gender was also one of the

variables that was considered. 4 of the participants that were deceived were male and 2 were female. However, because the sample is relatively small the division of gender could have been coincidental.

Conclusions and future work

Phishing attacks have been around for a while and even though companies are taking measures to decrease the risk of being affected by these cyberattacks they still fall prey of cybercriminals that aim to exploit the sensitive information of the company. More often than not, the weakest link to protection against threats are the employees and the human factor. Based on research, the most successful cyberattacks are the ones that target human's judgement and not the technical vulnerabilities of the systems.

As such, we saw fit to explore the susceptibility from phishing attacks in an Albanian Telecommunication company. We conducted an experiment and observed the behavior of 20 employees to see if they would respond to the phishing email and give their personal information. Also, we observed if whether they reported the suspicious email to their representatives. Based on the level of awareness, we concluded that informing employees about the phishing scams had a positive effect on protecting the company from such threats.

The aim of the study was to explore the behavior of the employees when confronted with phishing spams rather than hypothesize and generalize on a wider scale. The number of participants was limited to 20 and we are aware that it is a small sample. Further studies could benefit from a larger sample and a more diverse group of participants. We hope that we provided a good theoretical foundation and literature review as well as give a picture of how the employees' behavior when they become victims of social engineering and phishing scams.

References

Abassi, A., Zahedi, F. M., & Chen, Y. (2016): Phishing susceptibility: The good, the bad, and the ugly. 2016 IEEE Conference on Intelligence and Security Informatics, 169-174, Tucson: IEEE

Benenson, Z., Gassmann, F., & Landwirth, R. (2016): Exploiting curiosity and context: How to make people click on a dangerous link despite their security awareness, viewed 15 January 2018, retrieved from:

https://paper.seebug.org/papers/Security\%20Conf/Blackhat/2016/us-16-:

Benenson-Exploiti ng-Curiosity-And-Context-How-To-Make-People-Click-On-A-Dangerous- Link-Despite-Their-Se curity-Awareness-wp.pdf

Butavicius, M., Parsons, K., Pattinson, M., McCormac, A., Calic, D., & Lillie, M.

(2017): Understanding susceptibility to phishing emails: Assessing the impact of individual differences and culture. Proceedings of the Eleventh International Symposium on Human Aspects of Information Security & Assurance, 12-23

Caputo, D. D., Pfleeger, S. L., Freeman, J. D., & Johnson, M. E. (2018): Going spear phishing: Exploring embedded training and awareness. IEEE Security & Privacy, 12(1), 28-38

Chaudhry, J. A., Chaudhry, S. A., & Rittenhouse, R. G. (2016): Phishing attacks and defenses. International Journal of Security and its Applications, 10(1), 247-256

De Kimpe, L., M Walrave, W., Hardyns, L. Pauwels & K. Ponnet (2018): 'You've got mail! Explaining individual differences in becoming a phishing target. Telematics and Informatics, https://doi.org/ 10.10106/j.tele.2918.02.009

Gavett, B. E., Zhao, R., John, S. E., Bussell, C. A., Roberts, J. R., & Yue, C. (2017): Phishing suspiciousness in older and younger adults: The role of executive functioning. PLOS ONE, 12(2), 1-16

Gratian, M., Bandi, S., Cukier, M., Dykstra, J., & Ginther, A. (2018): Correlating human behaviour and cyber security behaviour intentions. Computers & Security, 73, 345-358

Mayhorn, C. B., Welk, A. K., Zielinska, O. A., & Murphy-Hill, E. (2015): Assessing individual differences in a phishing detection task. Proceedings of the 19th Triennial Congress of the IEA, Melbourne: IEA

Parsons, K., McCormac, A., Pattinson, M., Butavicius, M., & Jerram, C. (2017): The design of phishing: Challenges for researchers. Computers & Security, 52, 194-206

Sun, J. C. Y., Yu, S. J., Lin, S. S. J., Tseng, S. S. (2016): The mediating effect of anti-phishing self-efficacy between college students' internet self-efficacy and anti-phishing behaviour and gender difference. Computers in Human Behaviour, 59, 249-257

Talos (2018): Email & Spam Data, viewed 25 January 2016, retrieved from https://www.talosintellige nce.com/reputation center/email rep#global-volume