Chapter 3

Benefits of Information Security Awareness Training Against Phishing Attacks:

A Field Study

Arzu Tufan
Yıldırım Holding A.Ş., Turkey & Ahmet Yesevi University, Turkey

Gurkan Tuna
https://orcid.org/0000-0002-6466-4696
Trakya University, Turkey

ABSTRACT

Phishing attacks are human-targeted attacks, and it may not always be possible to counter them with technical measures alone. By their nature, humans have a natural weakness of desiring to believe. Cyber attackers who analyze this vulnerability well have been exploiting this in order to achieve success in their respective attack targets. This study focuses on reviewing the benefits of information security awareness training against phishing attacks and aims to provide insight on this through the results of a field study. The field work was carried out in Turkey on four different scenarios on the success of information security trainings against phishing attacks. The data obtained as a result of the field study were compared with the data obtained in international studies, and the maturity of the non-regulated institutions in Turkey against phishing attacks was measured. When the data obtained as a result of the field study were compared with the international results, it was evident that the test group subject to the study exhibited a success below the international values.

DOI: 10.4018/978-1-6684-7207-1.ch003

INTRODUCTION

Parallel to the rapid progress of digital transformation processes, crime and attack elements have also rapidly shifted to digital environments. Even today, attacks and wars have evolved into cyber wars and attacks (Sharma, 2010). Parallel to this, the most important target is the human being, the weakest point. Because the greatest weakness of man is belief, trust, curiosity and the belief that he can easily achieve what is difficult to achieve. This is where phishing attacks come into play, and attacks targeting corporate and personal information are created through scenarios that will use these vulnerabilities of human beings (Khonji, Iraqi, & Jones, 2013). As a result, not only individuals, but also corporations and organizations suffer. This situation causes especially financial, trust and prestige losses in corporations and organizations.

As methods used to realize phishing attacks have been becoming more and more sophisticated, different methods have been proposed to detect phishing. Karabatak and Mustafa (2018) stated in their study that users experience financial losses due to various threats in the Internet environment and that they refrain from shopping online for such reasons. They showed phishing websites as one of these threats and concentrated on this in their studies. The authors worked on the ready-made dataset from the UCI Machine Learning Repository (Dua & Graff, 2017). In order to achieve better performance in their work, they reduced the size of this ready-made dataset with feature selection algorithms. During their tests, they used many of the familiar classifications such as Bayesian, Bayesian, ID3 and noted the results. When they compared the results they obtained, they stated that the KStar algorithm gave the most accurate result with an accuracy of 97%. Chiew et al. (2018) used favicons to detect phishing websites in their study. The authors determined whether a website was original or a phishing one with the help of a complex mathematical formula. In their method, they searched the favicons on the websites in Google images. They also presented alternative methods for detecting phishing websites that do not contain favicons. Moreover, they added domain name system amplification feature to their work. Based on a set of favicons of 5000 phishing websites and 5000 real websites, they reached an accuracy rate of 96.93%. Ding et al. (2019) used search engine, heuristics and logistic regression to detect phishing websites. As a first step, the authors searched for the domain name of the website they were testing in the Baidu search engine. If the domain name was in the top 10 results, they decided that this website was legitimate. If there were no results in the top 10, heuristic rules was used as the second step and the content of the website was searched. If the suspicion of phishing persisted, logistic regression was used in the final step. At the end of these three complementary steps, the authors decided whether the website was phishing or not. In addition, they successfully detected phishing web site with an accuracy rate of 98.9%.

When cyber attacks are taken into consideration, it can easily be seen that phishing attacks have a very important place in the stage of establishing the first contact with the victims (Jansson & von Solms, 2013). However, since these attacks are directly human-targeted, technological measures alone do not provide benefits. Therefore, the most important defense mechanism is the human factor and its maturity level.

The purpose of this study is to measure the benefits of information security and cyber security awareness trainings against cyber attacks realized by phishing method. It is to evaluate the results obtained by comparing them with the studies conducted around the world. In this research, a total of 1200 participants working at 9 different sectors who received the necessary awareness training on information security and cyber security, fully understand, internalize and fully implement these trainings in their digital lives was included. Within the scope of this study, phishing e-mails prepared on four different topics were sent to

Related Content