8-10-2022

Analyzing User Behavior Against Phishing Emails

Hak Ju Kim
Hofstra University, hak.j.kim@hofstra.edu

Michael Nizich
Hofstra University, michael.nizich@hofstra.edu

Analyzing User Behavior Against Phishing Emails

TREO Talk Paper

Hak J. Kim
Hofstra University
hak.j.kim@hofstra.edu

Michael Nizich
Hofstra University
michael.nizich@hofstra.edu

One of the most common cyberattacks is phishing, which preys on unsuspecting users to click hyperlinks to activate malicious software (called 'malware'). A phishing attack is designed for the purpose of either damaging the victim's computer or more commonly, hijacking that person's computer to steadily relay personal information to a host. However, it is less understood what the various attributes and characteristics of a specific phishing attack are leading to successful execution of a malware attack. Rather, it is even less understood what types of human behaviors are leading to the initial allowance of this attack. The objectives of this study are to observe and identify the behavior of a participant (victim) during and after a phishing attack, and to understand the various behavioral characteristics of a phishing attack's victim. This study conducted an experiment to identify the various behavioral characteristics of a phishing attack's victim both during and after a successful phishing attack has been executed.

This study is designed to observe, capture, and collect a participant's behavior. The collected data will be analyzed. Multiple emails are randomly sent to the participant from outside sources that contain an active, harmless, embedded hyperlink to a hosted script that will execute upon the participant clicking the hyperlink. Some emails are malware phishing attacks and others are regular emails. A participant's behavior will be observed during and after a malware phishing attack. Observation of a user includes the visual and audible behavior of a participant through cameras, microphones, and the data is collected from participant activity on the experiment PC. A participant will be notified of a successful phishing attack via a message on their computer screen.

For the experiment, a total of 25 participants will be recruited, with their ages ranging from 19 to 65 years old in the Hofstra community including faculty, staff and students. To participate, subjects have to meet the condition that they currently use an email through a PC (desktop/laptop) device frequently, whether for personal and/or professional use.

This study will have three phases: phishing behavior experiment, participant questionnaires, and focus group interviews. Phase I: Phishing Behavior Experiment 5 participants at a time will be placed on computers and given access to a predefined email account that is representative of their account as a member of that organization. A series of 10 emails will be sent to each participant at varying time intervals over a 20 minute period. From the 10 emails, there will be 6 business related emails that require an immediate answer from the participant and 4 emails that will contain links to simulated, yet harmless, phishing malware attacks. Each of the 4 phishing emails, if the hyperlink is clicked by the participant, will culminate with a popup message on the computer that they have just activated the attack so the participant will clearly know their actions were responsible for the simulated attack.

The preliminary experiment results show that objects (participants) do not recognize well whether a received email is regular (benign) or spam (malicious) and they do not show distinctive emotional responses between benign emails and malicious ones. From the questionnaire data, they are concerned that their computers may have been affected by malicious emails and are familiar with some attributes of malicious emails, such as misspelled words, invalid email suffixes, and company logo-embedded emails.

Our study will contribute to give some indication that security awareness training is important to prevent and protect a user's computer and data from cyberattacks (e.g., malicious emails).

References

Alzuwaini, M and Yassin, A. 2021. “An efficient mechanism to prevent the phishing attacks,” *Iraqi Journal for Electrical & Electronic Engineering* (17:1), pp.183-194.

Arief, B., Periam, A., Cetin, O., and Hernandez-Castro, H. 2020. “Using Eyetracker to Find Ways to Mitigate Ransomware,” *6th International Conference on Information Systems Security and Privacy*.

Curtis, S., Rajivan, P., Jones, D., and Gonzalez, C. 2018. "Phishing attempts among the dark triad: Patterns of attack and vulnerability," *Computers in Human Behavior* (87), pp. 174-182.

McAlaney, J. and Hills, P. 2020. “Understanding Phishing Email Processing and Perceived Trustworthiness Through Eye Tracking,” *Frontiers in Psychology* (11), pp. 1-13.