Another Phishing Training - Role playing as an attacker

A Thesis

Submitted to the Graduate Faculty of the
University of New Orleans
in partial fulfillment of the
requirements for the degree of

Master of Science
in
Computer Science

by

Saroj Duwal

Bachelor in Science

University of New Orleans, 2019

May, 2022

Table of Contents

List of Figures

FIGURE Page

List of Tables

TABLE Page

1. Introduction

The rapid adoption of the internet in everyday life and work place has presented us with new security challenges. Users are more susceptible to attacks by malicious users on the internet. There are various technical security measures in place such as firewall, encryption, threat hunting software, and engaging automation to mitigate these challenges. However, studies have shown that the human layer is the weakest link in the security chain[1]. Attackers usually start by targeting the human link before carrying out other detrimental attacks. These attacks that are accomplished with human interactions are termed as social engineering attacks. The goal of such attack is to trick the victim into making security mistakes or giving away sensitive information.

The rapid adoption of the internet in the workspace and everyday life has presented new security challenges. Phishing attacks are one of the most common and well-known problems experienced by many organizations [2]. Phishing attacks are reported to be on the rise and unlikely to decrease soon. A report by Anti-Phishing Working Group (APWG) saw the number of phishing attacks has doubled from early 2020 [3]. A common type of phishing attack is a *click-jacking attack* that is designed to trick users into clicking on links that are not intended for them. Such links redirect victims to sites that are carefully designed to mimic those of legitimate businesses and services with the goal of convincing users to provide their personal information and credentials[2]. Effects of such attacks are hard to quantify all attacks may not be reported. Estimates of damage caused by phishing vary widely, ranging from $ 61 million per year to $ 3 billion per year [4].

Phishing attacks are often carried out as a starting point for other detrimental cyber-attacks[2]. Attackers ofter start by targeting the weakest link i.e. the human layer[1]. There are various technical security measures in place to prevent and filter out phishing emails[5, 6], but such systems are not perfect and cannot filter out all malicious emails.

Training the human layer is a critical step in preventing and filtering out phishing emails. There have been plenty of research on the best way to train the human layer. One of such prevalent way

of training the users are with the use of cyber security videos and tutorials. However, studies show that such resources work only if the users are paying attention to them[7]. To better engage the learner, several anti-phishing games have been proposed. Although, study shows that games have been successful in improving the users ability to detect spam links and websites, many games leave out the email context. Attackers might leverage these to demand immediate attention and encourage quick response. Attackers might use different techniques such as spoofing and present sense of urgency in the email to trick the users in clicking the email.

To develop an comprehensive training game, we have developed "game", a role playing simulation game. Role playing game to train users are not a novel concept[8], and have shown promising result. However, existing role playing games approach the training from the victim perspective. This might limit the emails they see and miss important details on what to look for. "Game" requires the player to act as an attacker and train different skills used to create phishing emails. Phishing emails are randomly generated (based on the attacker skills) from a set of templates collected from real phishing emails. Role playing as an attacker also allows us to concentrate on domains, and implement some mechanics to present how different domains and subdomains can be used to create phishing emails.

References

[1] A. Security, "The cost of cybercrime," tech. rep., Accenture Security, 2019.

[2] D. Jampen, G. Gür, T. Sutter, and B. Tellenbach, "Don't click: towards an effective anti-phishing training. a comparative literature review," *Human-centric Computing and Information Sciences*, vol. 10, no. 1, 2020.

[3] A.-P. W. Group, "Phishing acativity trends report 3rd quarter 2021," tech. rep., Anti-Phishing Working Group, 2021.

[4] J. Hong, "The state of phishing attacks," *Communications of the ACM*, vol. 55, no. 1, pp. 74–81, 2012.

[5] S. Hird, "Technical solutions for controlling spam," in *In proceedings of AUUG2002*, pp. 4–6, 2002.

[6] Z. Dou, I. Khalil, A. Khreishah, A. Al-Fuqaha, and M. Guizani, "Systematization of knowledge (sok): A systematic review of software-based web phishing detection," *IEEE Communications Surveys and Tutorials*, vol. 19, no. 4, pp. 2797–2819, 2017.

[7] P. Kumaraguru, S. Sheng, A. Acquisti, L. F. Cranor, and J. Hong, "Teaching johnny not to fall for phish," *ACM Transactions on Internet Technology*, vol. 10, no. 2, p. 1–31, 2010.

[8] Z. A. Wen, Z. Lin, R. Chen, and E. Andersen, "What.hack," *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, 2019.