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

Page

List of Figures 2

List of Tables 3

1. Introduction 1

References 2

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 an attack is to trick the victim into making security mistakes or giving away sensitive information.

Phishing is an example of social engineering attack in which a target or targets are contacted by email, telephone or text message by someone posing as a legitimate institution to lure individuals into providing sensitive data such as personally identifiable documents, banking and credit card details, and passwords[2, 3]. Phishing is part of a larger class of attacks known as semantic attacks. A "semantic attack" is an attack in which the attacker uses the computing infrastruture in a way that fools the victim into thinking they are doing something, but are doing something different, yet the computing system is working as intended. In the case of phishing, attackers exploit the fact that users tend to trust email messages amd websites based on superficial cues that actually provide little to no meaningful trust information[4]. Since attacks are ususally dependent on the information typed on a form, not malware infection of a computer, even a user with excellent can fall victim to these exploits.

References

[1] 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.

[2] KnowBe4, "What is phishing?."

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

[4] 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.