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 internet adoption in everyday life and the workplace has presented us with new security challenges. Users are more active on the internet, giving attackers more opportunities to attack unsuspecting victims. There are various technical security measures 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] and attackers usually start by targeting the most vulnerable link before performing other detrimental attacks. These attacks with human interaction are generally known as "Social Engineering Attacks" and use psychological manipulation to trick users into making security mistakes or giving away sensitive information.

1.1 What is phishing?

Phishing is an example of social engineering attack in which attackers target users by contacting them through email, telephone, or text message by someone posing as a legitimate [2, 3]. These attacks are challenging to detect as attackers use the computing infrastructure to fool the victim into doing something but are doing something else while the computing system is working as intended. Due to this, even users with a high-end security system can be victims. An example of such is the infamous case of John Podesta [4], Hilary Clinton's campaign chairman for the 2016 presidential election. The "googlemail.com" in the domain successfully tricked John Podesta and the Clinton campaign's computer help desk to trust the email(See fig:1.1).

Successful phishing attacks can be costly to an organization. For example, in 2020, attacks cost US businesses more than $1.8 billion, up from $1.7 billion in 2019 [5]. In addition, these attacks can also lead to credential/account compromise leading to leaks of sensitive information. In 2014, an attack was successful on an invasion of celebrity iCloud accounts, leading to the embarrassing leaking of nude photos. The leak was initially considered due to a breach on Apple services, but it was later a phishing attack pretending to be Apple and Google and asking them to change their

> *From:* Google <no-reply@accounts.googlemail.com>
> *Date:* March 19, 2016 at 4:34:30 AM EDT
> *To:* [redacted]ta@gmail.com
> *Subject:* *Someone has your password*
>
> Someone has your password
> Hi John
>
> Someone just used your password to try to sign in to your Google Account
> [redacted]@gmail.com.
>
> Details:
> Saturday, 19 March, 8:34:30 UTC
> IP Address: 134.249.139.239
> Location: Ukraine
>
> Google stopped this sign-in attempt. You should change your password
> immediately.
>
> CHANGE PASSWORD <https://bit.ly/1PibSU0>
>
> Best,
> The Gmail Team
> You received this mandatory email service announcement to update you about
> important changes to your Google product or account.

Figure 1.1: Phishing email sent to John Podesta

password [6, 7].

Phishing attacks have been continuously rising and have doubled since early 2020. In July 2021 alone, APWG saw 260,642 phishing attacks [3]. Additionally, Proofpoint found that more than 75% of organizations faced phishing attacks in 2021 [8]. These uprising trends in attacks have shown some serious need for mitigations for phishing attacks.

1.2 Current Mitigations

The prevention of phishing attacks can be divided into three steps [9]. The first step to stop a phishing attack is preventing the attack from reaching the end-user. We have seen multiple studies on phishing prevention with the help of the machine learning approach [10, 11]. Although these

models may catch some sites, it is impossible to filter out and prevent phishing attacks. The phisher can easily make a new site and learn to create better contextual attacks, preventing these models from being fully effective.

It is impossible to stop all the attacks as attackers usually design their attacks to reach vulnerable users. However, many web browsers and email clients are already prepared to warn users of any suspicious activities they detect. For example, browsers use active warnings such as "This page is not secure warnings" to warn the users of any certificates they fail to verify or pop up windows with a sign that the site they are on is suspected of forgery. In addition, there are other passive indicators, such as different shades of link highlights in the address bar, security lock signs, etc., that browsers use. Active warnings prevent more attacks [9], but attackers can easily bypass these warnings by creating new sites and new contextual websites.

Figure 1.2: Browsers uses different shades to indicate the primary link and the secondary links.

The final step to avoid phishing emails is user training. A study done by Proofpoint shows that 34% of US respondents believe emails with familiar logos are safe [8]. The study indicates a general lack of awareness about phishing campaigns among the general population. There are many tools used for phishing training. One of the most common tools to train users is cyber security videos. However, a study shows that these videos are only efficient only if the user pays attention through all of them [12]. We can also find other techniques such as reading materials and cyber security classes to raise awareness among users.

Although these training help users recognize phishing attacks, simply knowing does not provide helpful strategies for identifying phishing attacks. In addition, the lack of contextual information in these videos leaves room for improvement. Therefore, an interactive user program that conveys the information with a better approach is necessary. Our approach to using the game to

spread awareness tries to tackle this problem.

1.3 Litearature Review

The gaming approach to train users is not novel. Hendrix et al. [13] investigated whether games can be effective cyber security training tools with some of the popular games designed for cyber security training. Their study indicated positive signs, although there was insufficient evidence to draw definite conclusions.

subsectionEducational Games

1.3.1 Board Game

ctrlalthack

smells phishy

1.3.2 Phishing Link training

antiphishing phil

phish phinder - same as antiphishing phil

gamified approach - shooting game

1.3.3 Role playing game

what dot hack

1.4 Objective

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] "The phishing email that hacked the account of john podesta," Oct 2016.

[5] "Cybercrime statistics: Top threats and costliest scams of 2020."

[6] A. Duke, "5 things to know about the celebrity nude photo hacking scandal," Oct 2014.

[7] "Nude celebrity picture leak looks like phishing or email account hack," Sep 2014.

[8] 2021.

[9] I. Vayansky and S. Kumar, "Phishing-challenges and solutions," *Computer Fraud & Security*, vol. 2018, no. 1, p. 15–20, 2018.

[10] R. Yang, K. Zheng, B. Wu, C. Wu, and X. Wang, "Phishing website detection based on deep convolutional neural network and random forest ensemble learning," *Sensors*, vol. 21, no. 24, p. 8281, 2021.

[11] O. K. Sahingoz, E. Buber, O. Demir, and B. Diri, "Machine learning based phishing detection from urls," *Expert Systems with Applications*, vol. 117, pp. 345–357, 2019.

[12] 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.

[13] M. Hendrix, A. Al-Sherbaz, and V. Bloom, “Game based cyber security training: Are serious games suitable for cyber security training?,” *International Journal of Serious Games*, vol. 3, no. 1, 2016.