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

FIGURE Page

List of Tables

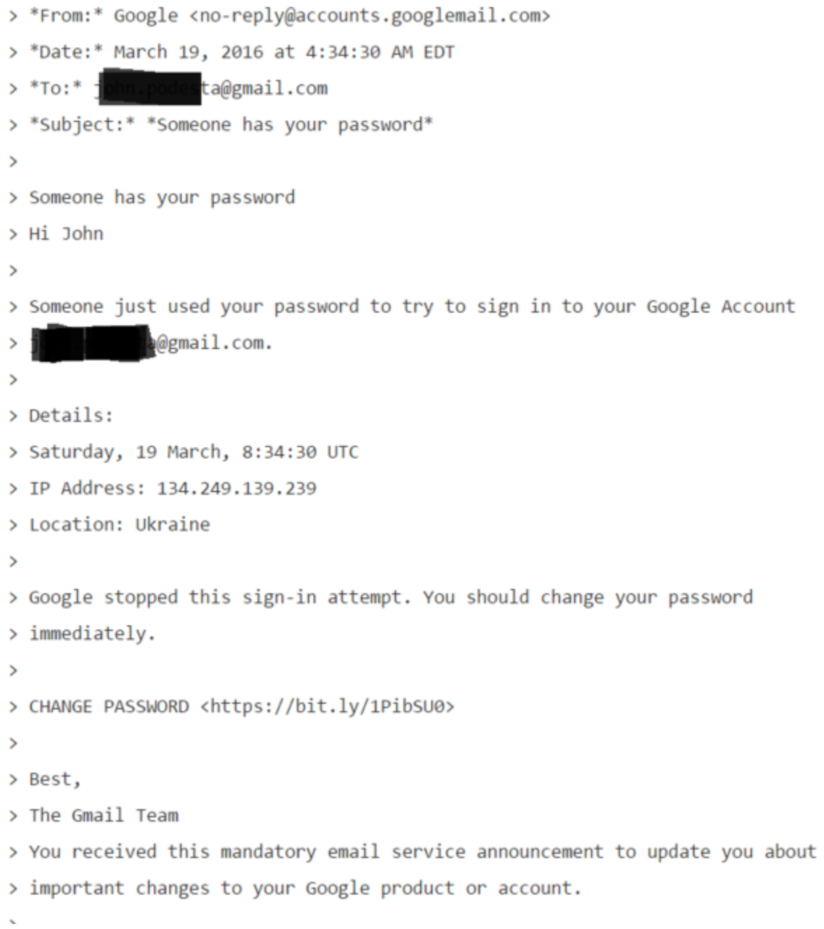
1. Introduction

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." Prevalent social engineering attacks such as phishing, pretexting, baiting, quid pro quo, and tailgating use psychological manipulation to trick users into making security mistakes or giving away sensitive information. This thesis will cover strategies to help people understand phishing and different detection techniques through our role-playing gameplay.

1.1 What is phishing?

Phishing is one of the most prevalent social engineering attacks in which attackers target users by contacting them through email, telephone, or text message by attackers posing as a legitimate entity [2, 3]. Unfortunately, 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).

Phishing attacks are constantly evolving with different tricks. For example, although Podesta's email shows it was initially generated from "googlemail.com," making it seem like it might be from Google, that might not be true. Attackers can use different spoofing techniques to hide the sender's identity. Another common trick attackers use (also present in Podesta's email) is to confuse the user with links hidden behind some text/button or confuse the user with redirecting links (example: TinyURL). As a result, the displayed text/link might not be the final destination. Podesta's team's failure to deal with this phishing email led to leaks of more than 11,000 emails which included private conversations with 2016 presidential nominee Hillary Clinton [5].



```
> *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

Successful phishing attacks are very costly to organizations. In 2020, phishing attacks cost US businesses more than $1.8 billion, up from $1.7 billion in 2019 [6]. These attacks can lead to credential/account compromise, giving the attacker access to sensitive information. Attackers may try to use these data for extortion. For example: 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 password [7, 8].

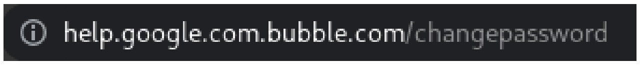
Phishing attacks are continuously rising and have doubled since early 2020. In July 2021 alone, APWG saw 260,642 phishing attacks [3]. Additionally, Proofpoint found that more than 75% of organizations faced phishing attacks in 2021 [9]. These uprising trends in attacks have shown some serious need for mitigations for phishing attacks.

1.2 Current Mitigations

The prevention of phishing attacks can be divided into three steps [10]. 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 models [11, 12]. Machine learning approaches such as K-nearest, XGBoost, CNN, RCNN, Random forest, etc., are commonly used to detect patterns and generalize phishing attacks. Some of the models have shown promises with more than 90% accuracy—however, a study conducted by What.Hack has shown that only one of the ten anti-phishing tools tested was able to identify over 90% of phishing websites correctly, and that tool also incorrectly identified 42% of legitimate websites as fraudulent [13]. Moreover, attackers are always looking for the best way to bypass these automated systems and develop new techniques if automated systems start flagging their attacks. The evolving nature of phishing attacks calls for an additional layer of security on top of the prevention layer.

If the attacks reach the user, the next step to secure the user is by warning the user. Most modern web browsers and email clients warn users of any suspicious activities they detect. For example, the browser will actively warn users with pop up for probable phishing sites. In addition, browsers provide passive hints to understand links better. Browsers use different shades of white to inform the user about a "fully qualified domain name (FQDN)" (also called absolute domain name), the complete domain name for a specific host on the internet. Figure 1.2 shows a use case for such a hint. Attackers will intentionally have a confusing link to trick users into clicking the link.

For example, although "help.google.com.bubble.com/changepassword" seems like an email from Google, the actual domain is bubble.com. Users can add any subdomain to domains they own, such as help.google.com.bubble.com, which can potentially be used in phishing attacks.Modern email clients provide similar hints for spam emails and notify the users if they can not verify the sender. Active warnings are more effective than passive signs [10], but attackers can easily bypass these warnings by creating new sites and context-aware websites or emails every time they are flagged.



ⓘ help.google.com.bubble.com/changepassword

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

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 [9]. 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 and reading materials. However, Kumaraguru et al. saw that users seldom seek these materials and tend to ignore emails directing them to these materials [14]. In addition, they noticed that most users do not spend much time reading security-related tutorials. This calls for an interactive training program to keep the user focused and engaged during training.

We have seen new and existing training materials incorporating gaming techniques. Gamification has been gaining rapid popularity over the past decade[15]. It increases engagement by incentivizing learners to pay attention and complete activities. We can observe existing training videos incorporating gaming techniques, such as letting users choose the correct option in the middle of training videos (a mini quiz game) and giving badges after completion. Newer training videos take gamification further and let learners play through various scenarios, make choices and see the rewards or consequences of their decision. For example, Infosec's Choose Your Own Adventure Security Awareness Game[16] has interactive storytelling to keep the user focused till the end of the video.

Gamification has improved the interactivity with the user, but existing training videos fail to cover the technical details that are commonly found in phishing emails. Our gameplay covers various technical aspects commonly found in phishing emails, such as domains, spoofing, and link hiding techniques attackers use to trick users.

1.3 Litearature Review

The gaming approach in education endeavors is not novel and has been used for over a decade [17]. There have been arguments for gaming in education. Prensky [18] in "Digital game-based learning" shows that playing "action" video and computer games has a positive impact on enhancing students' visual selective attention. He further argues that video games are the best opportunity to engage kids in real learning. This argument was further studied by Almeida [17] and verified that when games are used against the control group, significant increases in factual knowledge occur.

Several studies have used different gaming approaches to train phishing campaigns again. Hendrix et al. [19] 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. We will look at some popular work below, separated by category.

1.3.1 Board and card games

There have been some studies based on non-computer-based games. For example, Control-Alt-Hack [**?**] tries to educate the user with the help of a card game. Similarly, "Smells Phishy?" is another non-computer-based game that tries to raise awareness about online phishing scams. Both these game depends on cards to divide the task and learn skills. Although both the games had shown promise in their approach, non-computer-based games have some inherent limitations. The games require pre-setup (with the need for the cards and boards) and make it harder to use than computer-based games. Furthermore, the current approaches only teach users about phishing attacks. The limited skills these games provide may not be best suited as an individual training module.

1.3.2 Phishing Link training

There have been numerous computer games about phishing. One common category many studies focus on is training users to verify phishing links. Anti-Phishing Phil [?] is one of the pioneers in this field. Their gameplay puts the user as a fish. The goal of the fish is to grow larger by eating the good bugs (non-phishing links). Phish Phinder [?] is another example of link based training game that has similar gameplay and story to Anti-Phishing Phil but builds upon the game with more levels and interaction. Baral et al. [?] has a similar concept with a balloon shooting game. The goal of these games is to differentiate the phishing links and actual links. However, these games do not consider the context of the email. Attackers use psychological manipulation such as creating a sense of urgency, fake giveaways or making it seem like an email from somebody you know to trick people into clicking these links.

1.3.3 Role playing game

"What.Hack" [13] saw the shortcomings of the link-based game and developed gameplay that train the user on links as well as email context. "What.Hack" puts the user as a player required to process emails to acquire contracts and protect their network from cybercriminals. It approaches the training by having the user role play as a victim and look at different techniques that could be found in actual attacks.

The contextual emails addressed one of the most significant shortcomings of link-based games. The game successfully educated users with similar concepts as link-based games and added context to the links. The result from "What.Hack" clearly shows users' preference for their gameplay compared to Anti-Phishing Phil. Moreover, the game demonstrated significant improvement compared to other games in detecting phishing emails [13].

1.4 Objective

"What.Hack" clearly demonstrated that role-playing games with contextual emails were more effective than existing gameplays. Unfortunately, we could not find any other significant study that tried to build upon this finding. Therefore, we have developed gameplay inspired by "What.Hack" but approached the role-playing aspect as an attacker instead of a victim.

General phishing training such as videos and reading materials has taught users what to look for as victims. However, we believe looking at the attacker's perspective will help users understand what the attacker might look for while creating a phishing email. This will also help complement the currently available training games.

Our goals for the study can be summarized as:

- Develop a role-playing game to train the users about phishing through an attackers perspective
- Compare our results with the existing study

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] M. Anderson, “Wikileaks releases more purported emails, bringing total to more than 11,000,” Oct 2016.

[6] “Cybercrime statistics: Top threats and costliest scams of 2020.”

[7] A. Duke, “5 things to know about the celebrity nude photo hacking scandal,” Oct 2014.

[8] “Nude celebrity picture leak looks like phishing or email account hack,” Sep 2014.

[9] 2021.

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

[11] 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.

[12] 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.

[13] 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.

[14] 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.

[15] T. Schultz, “Gamification - cybersecurity’s turn to play,” Dec 2021.

[16] “Choose your own adventure security awareness games,” Jan 2022.

[17] L. C. Almeida, “The effect of an educational computer game for the achievement of factual and simple conceptual knowledge acquisition,” *Education Research International*, vol. 2012, p. 1–5, 2012.

[18] M. Prensky, “Digital game-based learning,” *Computers in Entertainment*, vol. 1, no. 1, p. 21–21, 2003.

[19] 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.