Social Engineering Attacks:

Phishing

Capstone Project

Submitted to: TEDPRIME

In Partial Fulfillment of the Requirements of the Cybersecurity July 15- September 14 Class 2024

Presented By

Omokhepen O. Gbolade

08/2024

INTRODUCTION

Social engineering refers to the various ways in which cybercriminals manipulate people into divulging confidential information or granting unauthorized access to their personal space or devices. However, I will be focusing on PHISHING, one of the most prevalent forms of online scams encountered in our daily activities. According to Cisco.com, “phishing is the practice of sending fraudulent communications that appears to come from legitimate and reputable source, usually through email and text messaging. The attacker’s goal is to steal money, gain access to sensitive data and login information, or to install malware on the victim’s device”.

This research aims to present the best awareness strategy for social engineering, that is, how to identify and avoid cyber-attacks. To achieve this, a malicious link was first created using the website bitly.com, followed by a focus group with colleagues from my church's WhatsApp platform. In this group, I conducted awareness training on social engineering focusing on phishing, and how to identify and avoid it. I then indirectly sent the malicious link to the group and evaluated how they reacted to it to test whether the awareness training was effective.

Below is a step-by-step process, findings on social engineering awareness training, and an analysis of how effective the strategy was.

1. Creating the malicious link

For this project, a malicious link was created using the bitly.com website platform. First, an account was created, which leads to the landing page menu, on the heading it shows Create new, you will click page, which leads to the building and design of the malicious link, it was then published for easy tracking.

The first link created was to lure the group into clicking the link to send birthday greetings to the founder of the church. The same process was used for the second link and the link generated was for them to send their information for a children’s Teacher Training. See the links below.

* <https://bit.ly/m/winnerschapelpapa70thbirthdaycelebrate>
* https://bit.ly/m/Winnerschapelchildrensteachertraining

A screenshot of a computer

Description automatically generated A screenshot of a computer

Description automatically generated

A screenshot of a phone

Description automatically generated A screenshot of a computer

Description automatically generated

A screenshot of a cell phone

Description automatically generated

1. Awareness

An awareness training was conducted using the focus group created and most of the things below were shared to inform them on how to identify and avoid phishing scams. At one point or another, we have received emails, text messages, and even calls requesting that we click a link, send a code, or enter our confidential information. This type of cyberattack is called phishing. Unfortunately, many people still fall victim to these scams because they are not patient enough to verify information before acting or not aware of ways to avoid it.

There are tips to identify and avoid phishing scams. These include, but are not limited to:

• What we call the zero-trust principle. This simply means you don’t trust any messages, emails, or calls until they are verified.

• Verify the sender’s email address—most businesses will use their domain names (e.g., Faithtabernacle.org).

• Don’t be in a hurry to click any link, no matter how real it looks.

• Be careful with your personal or confidential information. That’s why your banks will tell you, “We won’t ask for your PIN or password.”

• If you feel your information is compromised, quickly reset your password and alert your bank and other institutions.

• Update your devices’ software regularly. You can put it on auto-update.

• Use strong passwords and do not save your information on your phones. A password manager can help with storing your passwords.

▪︎ Use two-factor authentication on your devices.

Following these tips can help avoid having leaked information.

A screenshot of a chat

Description automatically generatedA screenshot of a chat

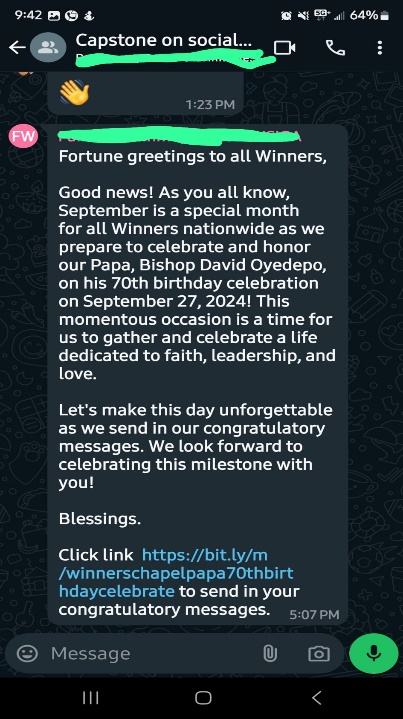
Description automatically generatedA green screen with white text

Description automatically generatedA screenshot of a phone

Description automatically generated

1. Findings

The first malicious link created was then posted on the group a few hours later after the training and these findings below were the results. Out of a total of 19 active participants, seven members from the group and three outside the group still fell victim to the assumed malicious link. I presumed someone from the group forwarded it to their friends outside the group because it shows a different location(Nigeria).

 A screenshot of a phone

Description automatically generated A screenshot of a phone

Description automatically generated

A screenshot of a phone

Description automatically generated A screenshot of a phone

Description automatically generated

The second awareness training was then conducted after sharing findings with the group, more information on how to avoid being scammed was sourced from us.norton.com. It was more like a reminder to the participants that no matter how real any messages or links look, they must be verified or else they will continue to fall victim to scammers out there. The second malicious link regarding church training was then posted.

A screenshot of a chat

Description automatically generated A screenshot of a computer

Description automatically generated A screenshot of a chat

Description automatically generated A screenshot of a social media post

Description automatically generated A screenshot of a cell phone

Description automatically generated

1. Conclusion

Knowing fully well that these attackers always devise new ways to scam people, the best strategy to avoid or minimize these social engineering attacks is for organizations to conduct regular awareness training and testing for their employees.

**References**

* Us.norton.com <https://www.cisco.com/c/en/us/products/security/email-security/what-is-phishing.html>
* Cisco.com <https://us.norton.com/blog/online-scams/what-is-phishing#:~:text=Ending%20the%20interaction%20after%20clicking,you%20clicked%20a%20phishing%20link>