Phishing: Analysis & Prevention

CIS 454 Final Project

Esmeralda Xhyliu  
Department of Electrical Engineering and Computer Science  
 Cleveland State University  
 Cleveland OH USA [2752750@vikes.csuohio.edu](mailto:2752750@vikes.csuohio.edu)

Nathanael Ahiagbedey  
 Department of Electrical Engineering and Computer Science  
 Cleveland State University  
 Cleveland OH USA [2755225@vikes.csuohio.edu](mailto:2755225@vikes.csuohio.edu)

Alexandru Lechintan  
Department of Electrical Engineering and Computer Science  
 Cleveland State University  
 Cleveland OH USA [2752803@vikes.csuohio.edu](mailto:2752803@vikes.csuohio.edu)

Asma Altabbaa  
 Department of Electrical Engineering and Computer Science  
 Cleveland State University  
 Cleveland OH USA [2770016@vikes.csuohio.edu](mailto:2755225@vikes.csuohio.edu)

ABSTRACT

Within this paper, we discuss the process of analyzing the ease and danger of phishing. Phishing is a type of attack that a user might receive through their email service. The email usually attempts to ‘bait’ the user into clicking a link and performing an action. When this action is completed, the attacker may steal personal information or attempt to deploy malware onto the user’s machine. Within our project, we developed our very own safe ‘phishing’ email that would direct users to click on a link within their Cleveland State University emails. This link would redirect the user to a CampusNet counterfeit where, when the user attempted to login, they would be notified that they had been ‘phished’. No personal information was gathered but the number of views and users on our website was gathered to show the dangers. To help create a solution, we developed a chrome extension that would keep track of visited sites the user interacts with and allow the user to mark them as trusted site. These trusted sites are maintained in a firebase database. When the user would access an untrusted site, the website would then be blocked and stated as a “phishy site”

1. Introduction

Phishing is a cyber-attack sent through an email where users are usually lured to click on a link. This link might redirect to a counterfeit of a familiar site for the user, or even cause a download of malware to begin. According to the Verizon Data Breach Report 2022, “Phishing remains one of the four main entry points to an organization, accounting for more than 60% of all social engineering attacks.” Showing that even large-scale corporations are attacked like this. A tactic as simple as a familiar email, with a recognized name or corporation can convince someone to either send an email in return or merely deceiving them into clicking a link. Through this process attackers can steal login credentials, credit card information, and even in extreme cases access a user’s computer. The problems with the phishing attack are it is difficult to trace back to the source, it can cause users financial damage, and for businesses, they can lose the trust of their customers.

For such a simple attack that can be done by anyone, are there any solutions or ways to help prevent this? Antivirus software and firewalls can help prevent malware. DNS filters can help stop you from going to untrusted sites, are some ways to help. The most important and simplest way is to be aware of where an email is coming from and the content it contains, everything from the email address to the specific font and size used could help.

2. Design & Analysis

When creating our CampusNet ‘dupe’ we attempted to use similar HTML and CSS code as close as possible to the original to provide as best of an illusion as possible. To even further the illusion, a domain of “campusnetcsuohio.com” was purchased to rival that of the original “campusnet.csuohio.edu”. This domain was purchased through google domains. A careful examination of this domain will reveal to the inspector that our fake domain name is missing a period between the phrase “campusnet” and “csuohio”. Yet to most unexpecting individuals this is a small enough of a difference to not raise any alarms.

Graphical user interface, website

Description automatically generated

Figure 1: Counterfeit Campuset

With our new domain we created an email to resemble that of the “Viking Store”. Google domain offers an option to also create an email from the purchased domain name, so we were able to take advantage of that as well. We decided to mimic the Viking store due to the caution banner that is placed on emails which did not originate from inside the CSU email servers. Emails from the Viking store is also tagged with this caution banner. Therefore, this would appear to be more believable to anyone who was patient enough to question why the banner was there.

Text

Description automatically generated

Figure 2: Phishing Email

Then replicating a previous email from April of 2022, we sent an email notifying students of the CIS 454 class that they had received a free $100 on their Viking ID Card, and to activate it they must login to CampusNet using our link. When these users read the email and clicked the link, they arrived at our landing page, an exact duplication of the true CampusNet created by Cleveland State University themselves. Once attempting to click the login page, users would be redirected to a page with a dancing fish on a hook and the words “You’ve been Phished”. As depicted in Figure 3: “You've been phished”

A picture containing text

Description automatically generated

Figure 3: “You've been phished”

When creating our landing page, and phishing page, we included a tag from Google Analytics. Using these tags, we were able to view how many users accessed our sites, both the landing page and phishing pages individually. We could also see how many times each page was viewed, the average engagement time on each site, the number of scrolls per page. Below is an example of what the tags could show us. Figure 4:

Chart, line chart

Description automatically generated

Figure 4: Analysis of Users, and Page Events from Google Analytics

The data shown would be able to show us a timeline of when users accessed our website. The phishing email was sent on November 29th, 2022. As you can see on that specific day, the number of users reached a peak and then immediately died down once users began to see the phishing page and notified their classmates. This page from Google Analytics shows the overall number of users accessing, New vs. Returning. The average engagement time, and the total event count, meaning page scrolls, clicks and views. Also using google analytics we’re able to analyze views on specific pages as seen on Figure 5:

Graphical user interface, application

Description automatically generated

Figure 5: Analysis of the specific views per page using Google Analytics

After receiving our data from the Google Analytics pages and seeing the actual numbers, we contemplated developing a possible solution that could reduce the amount of phishing attacks. For our selected solution, we decided to develop a simple Chrome Extension. This chrome extension, when downloaded and installed will allow users to have a database that contains a list of trusted sites. When the user accesses any of the sites that are part of their trusted sites list, they are able to use it as intended with no changes, however when the user accesses a website that is not on the list, they are prompted on whether or not they would like to add that site to their trusted list. If the user selects yes, then they will be able to proceed to the newly trusted site. However, if the user selects no, to not add the website to their database, then when refreshed, the page, will display a block stating “phishy site”. As displayed in Figure 6 shown below.

Graphical user interface, text

Description automatically generated

Figure 6: Blocked Site

This will stop the user from accessing anything on the website to protect them from the harms of a phishing site. This example of a chrome extension would be very useful in the situation that we created. Where users access the “campusnet.csuohio.edu” website very frequently knowing that any other similar domain would be a fake. The user would be able to add the real domain to their trusted sites and the fakes would then show that they are untrusted. If the user mistakenly adds an untrusted site to the list of trusted sites, we’ve offered them an option to remove this site from the database.

Graphical user interface, website

Description automatically generated

Figure 7: Removing Site from Database

3. Evaluation

Using Google Analytics as stated in the above section we were able to evaluate and analyze how many students in our class could be phished. According to our data we had 73 users access our website with 67 of the users being new. The returning users were our group members for testing purposes. The 67 users are more than the number of students that we have in our class, meaning that our phishing email may have been forwarded to friends of CIS 454 students, or quite possibly our domain name was so close to the original campus net address that users may have accessed it through looking it up on a search engine. Of the users that accessed, analytics showed that we had 99 views on our original landing page, which was the CampusNet dupe. Then on our phishing page, we received 45 views. Showing that about 45% had been “phished” by us. Also, we could see that the average engagement time was 6 seconds, showing that users may have logged on, seen that it was fake by our phishing page and then quickly logged off to attempt to prevent anything bad from happening.

4. Roles

This project was made possible in large part to our collaborative discussions and group creativity. Since none of us had experience in creating chrome extensions or is trained in social engineering best practices. It was difficult to designate a specific role to each individual. Rather we discussed and adapted to suggestions and solutions that were offered by each member. Therefore, we’ve listed below general categories that each member played the greatest role in.

Asma:

* Find possible solutions to prevent phishing
* Develop Phishing Prevention Chrome Extension
* Create Phishing Email

Alexandru:

* Gather data by using Google Analytics
* Develop Phishing Website
* Implement Google Tags

Esmeralda:

* Find possible solutions to prevent phishing
* Develop Phishing Prevention Chrome Extension
* Create Phishing Email

Nate:

* Gather data by using Google Analytics
* Develop Phishing Website
* Implement Google Tags

CONCLUSION

In conclusion, for our CIS 454 Networks Final Project, we decided to show the ease of manipulation and danger that is Phishing. We did this by developing our very own CampusNet dupe website which redirected users, when they attempted to login, to a page that notified them that they had just been “phished”. A link to this email was sent to all the CIS 454 Networks students stating that they had just been gifted $100 on their Viking ID where they must login to CampusNet through that link to redeem it. The interactions to the website were all tracked using Google Analytics. With this, we were able to see how many users accessed each page and how long they spent. We discovered that more students than were in the networks class accessed the site. Also, about 45% of the views on the site made it to the phishing site. To help show an example of a solution to the problem of phishing, we developed a Chrome Extension that allows users to create a database of their trusted sites. When the user accesses any site that was not on their list, they would then get prompted to add it to the list. If this suggestion was denied, then the page would be blocked. This would help users to not access websites that are counterfeits, as the originals would be added to their trusted site database.

REFERENCES

[1] “Verizon Data Breach Investigations Report (DBIR) - 2022,” *Phishing Simulation & Cyber Security Training*. [Online]. Available: https://www.phishingbox.com/news/post/verizon-data-breach-investigations-report-dbir-2022. [Accessed: 08-Dec-2022].

[2] “Phishing facts,” *Statistics Security & Data Breaches*. [Online]. Available: https://www.phishingbox.com/resources/phishing-facts. [Accessed: 08-Dec-2022].

[3] M. B. A. Jason Firch, “How to create an email phishing campaign in 8 steps,” *PurpleSec*, 24-Oct-2022. [Online]. Available: https://purplesec.us/phishing-campaign/. [Accessed: 08-Dec-2022].

[4] “Firebase Realtime Database,” *Firebase*, [Online]. Available: https://firebase.google.com/docs/database

Conference Name:ACM Woodstock conference

Conference Short Name:WOODSTOCK’18

Conference Location:El Paso, Texas USA

ISBN:978-1-4503-0000-0/18/06

Year:2018

Date:June

Copyright Year:2018

Copyright Statement:rightsretained

DOI:10.1145/1234567890

RRH: F. Surname et al.

Price:$15.00