SOCIAL ENGINEERING ATTACK: E-MAIL PHISHING SIMULATION[1]

Tolga Emre Koraş[1], Supervisor Prof. Dr. Emre Olca[2], Emin Mert Demirci[3]

[1]Maltepe University, Faculty of Engineering and Natural Sciences, Istanbul / Türkiye

[2]Maltepe University, Faculty of Engineering and Natural Sciences, Istanbul / Türkiye

[3]Maltepe University, Faculty of Engineering and Natural Sciences , Istanbul / Türkiye

Abstract: This project dives into the E-mail phishing, a prevalent form of social engineering attack, with the objective of both observing and understanding the mechanics and evolution of these increasingly common attacks. The central goal is to build crucial awareness among the general populace about the nature of E-mail phishing, its current trends, and potential safeguarding strategies. By leveraging an interactive and user-friendly system, this project offers a hands-on learning experience. It is carefully designed to be accessible and understandable to all users, irrespective of their technical background. Participants engage directly with the process, entering a specially crafted website that hosts a variety of simulated phishing email templates. These templates, drawn from a database, represent common phishing tactics. Users initiate a simulated E-mail phishing attack using these templates and then observe its operational mechanics in real-time. This practical approach provides invaluable insights into the phishing process, demonstrating how such attacks are formulated and executed, and the subtle cues that can betray their tricky nature. Furthermore, the project aims to stimulate critical thinking about protective measures against such cyber threats. By analyzing data and trends from these simulated attacks, users can develop a deeper understanding of phishing strategies and lead a more vigilant and informed online presence. Ultimately, this project serves as a vital educational tool in the ongoing battle against cyber threats, empowering individuals with the knowledge and skills to protect themselves in the digital age.

Keywords: *E-mail phishing, Social engineering attack, Cyber threats, Educational tool, Safeguarding strategies*

INTRODUCTION

This study was produced from the "Course Project" of the first and third authors, of Maltepe University Faculty of Engineering and Natural Sciences, where the second author is an advisor teacher. ORCID ID: 0009-0001-4696-4134.

RELATED WORKS

Under the heading of cyber security, multiple studies have been conducted to raise people's awareness about social engineering and phishing attacks. Different projects developed for the same purposes as ours will be discussed.

In march 2009 A study paper, theory model published[3],Between 50%-70% of security incidents originate from within the organization. Because people/employees do not know how to use information systems properly. When we look at the research conducted, it was determined that the users did not have information about cyber security policies in the information collected from a total of 269 computers of 8 different companies, and that employees should receive training and be informed about cyber security. In our project, it is aimed to make the first-person experience and raise awareness based on the issue of Email phishing, which is one of the cyber security problems that is very popular today and still continues to increase in popularity, since other people, not a specific community, need to be aware of these issues.

In the project published[8] in 2020 IEEE 13th International Conference on Developments in eSystems Engineering (DeSE), The email phishing training website aimed to help users/people get knowledge on phishing. The project consists of interactive learning not first-hand observation. In our project, we offer end-users the to start a phishing attack firsthand and observe the process, get an idea, and gain a piece of knowledge about this growing cyber threat.

PURPOSE

This project focuses on the use of Email phishing, which is a dominant form of social engineering attack. The main aim of this endeavor is to gain an understanding to the common people about the progress and methodologies of Email phishing, which is a phishing tactic that has gained very significant attention in today's world and is showing a constant increasing trend. By observing the details of how these phishing attacks occur, we aim to gather important information about their general patterns and aim to help ordinary people improve themselves by seeing first-hand how these attacks work. This information obtained will be effective in developing preventive measures against such attacks. The project specifically focuses on learning the mechanics and details of phishing Emails, their structure, distribution, making ordinary people aware and understanding the manipulations they use to deceive recipients. This will allow us to not only identify but also predict potential phishing strategies, thus strengthening our ability to counter this ever- evolving cyber threat. The user who logs in to the system via the web browser must first create an account. After creating an account, you can enter the e-mail manually by selecting one of the fake target e-mails from the management page, or you can use the ready-made e-mail templates to reach a certain audience with the sorting feature. By selecting it, a sample phishing attack is launched. Selected templates, selectable emails and the information to which the emails are linked are stored in the database and retrieved from there. The victim, who clicks on the link in the sent e-mail, is directed to the fake web page created for the selected template, and the victim's information is stored in the database after being "stolen". The database is automatically updated.

SCOPE

Social engineering attack: Email phishing system consists of 3 parts that work together. These parts are WEB site, Visual Studio and Microsoft SQL server Database systems. The WEB site allows users to create and register accounts and log in to the Email phishing system using the accounts they create. By using the Management page, they can choose one of the available fake Email templates, manually enter the email address they have determined as the target, select one of the emails registered in the database, or perform phishing to a certain audience. Victims who click on the links in the fake emails sent are directed to fake websites in the selected template format and their information is stolen, and the stolen victim information is sent to the database for storage. Using the report page, one can observe the compromised victim information stored in the database. The database stores ready-made fake email templates, user-created account information, and stolen information collected from victims. Visual Studio hosts the html, Css and Javascript codes of the WEB site, allowing us to establish and manage the website and the connection between the database and the website.

METHOD

WEB Site: It is a site where end-users (ordinary people) obtain information and awareness about how the phishing method works, from the attacker's perspective, and initiate attacks. This site consists of 5 pages: log-in page, registration page, management page, report page and e-mail page. On the log- in page, if the user already has an account, he/she logs in to his account. If the end-user does not have an account, he/she registers on the sign-up page. On the e-mail page, he/she can view ready-made e-mail templates. On the Management page, he/she initiates a phishing attack. On the Report page, he/she sees the victim's information taken from the database.

Visual Studio: In Visual Studio ASP.Net framework is used to manage HTML, CSS and JavaScript codes. The connection between the website and the database is established and managed here. Simply put, most of the back-end and front-end are organized and realized in Visual Studio. Only admins have access to this section.

Microsoft SQL Server: Microsoft SQL server is used as the database. The end-user's user information is stored here. The information shown on the report page is pulled from here. Information stolen/taken from the victim is stored here. Visual Studio has access to the database. End-user does not have access to the database, only admins have access permission.

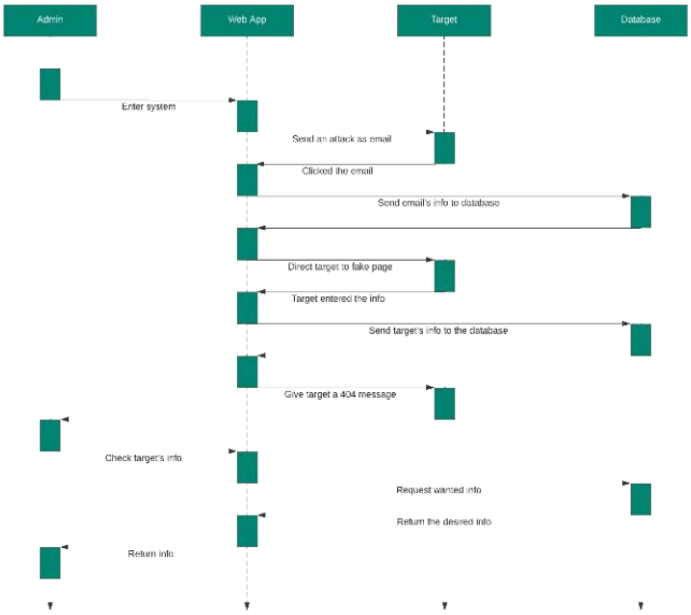


Fig. 1. The Sequence Diagram of Project

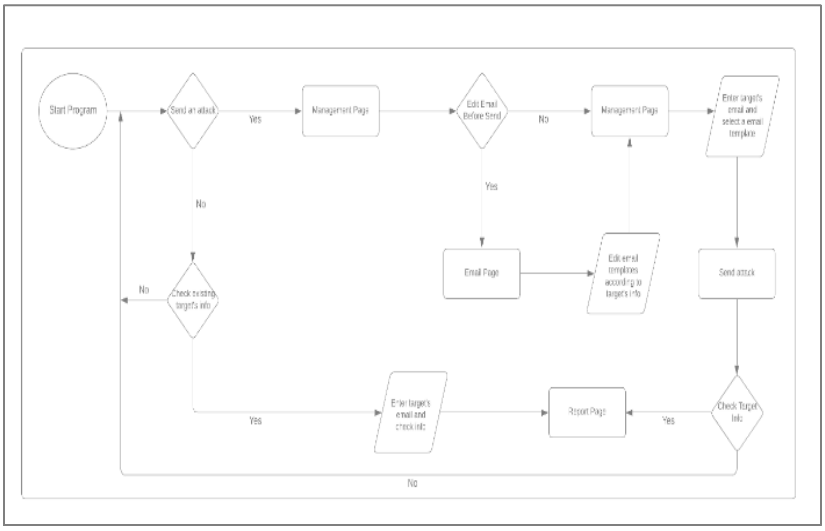

Start Program
Send an attack
Yes
Management Page
Edit Email Before Send
No
Management Page
Enter target's email and select a email template
Yes
No
Email Page
Edit email templates according to target's info
Send attack
No
Check existing target's info
Yes
Enter target's email and check info
Report Page
Yes
Check Target Info
No

Fig. 2. The UML Activity Diagram of Project

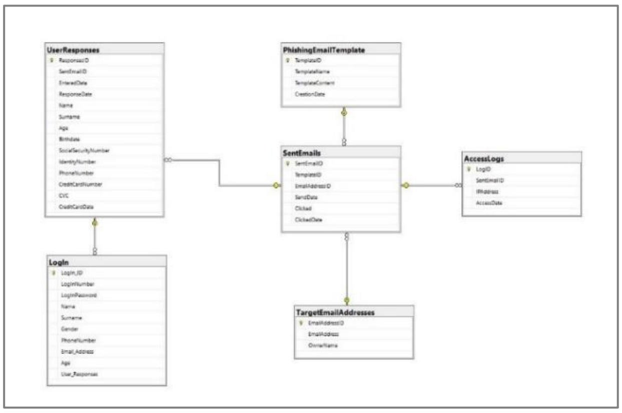


Fig. 3. Database Diagram of Project

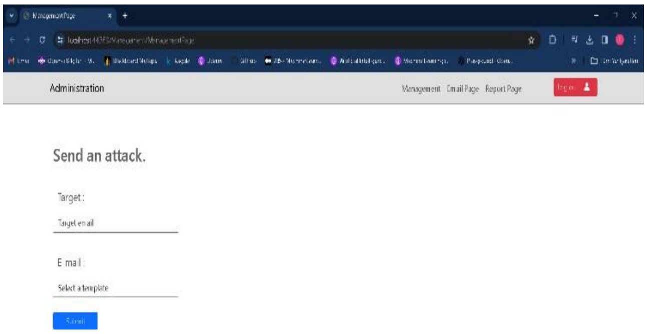
KEY FINDINGS

When we observed the people we selected who had no knowledge about this subject, it was observed that their awareness increased after they made the simulation and they decided to do research on this subject.

CONCLUSION

In conclusion, this project offers an approach to understanding and raising awareness about email phishing, a common type of social engineering attack. It aims to raise public awareness of how these phishing tactics work. Through a web-based system, users can experience the phishing process from the attacker's perspective, thus improving their awareness and ability to recognize such threats. Consisting of various pages such as login, registration, management, report and email template pages, this system allows users to simulate phishing attacks in a controlled environment. The backend and frontend of the website are managed using Visual Studio and ASP.Net framework, ensuring safe and efficient operation. Additionally, Microsoft SQL Server is used for secure data storage and retrieval, accessible only to administrators.

PICTURES OF SYSTEM



Send an attack.

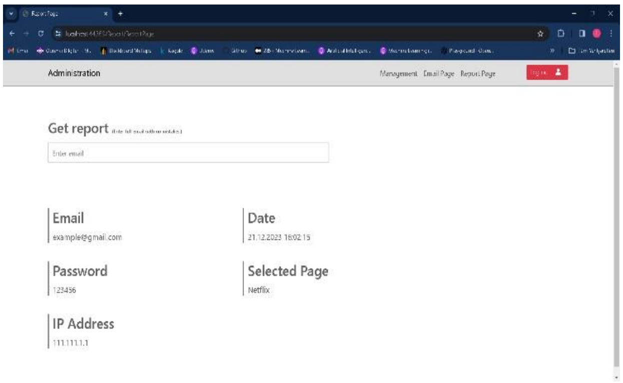
Target :

Target email

E mail :

Select a template

Fig. 4. Management Page



Get report

Enter email

Email
example@gmail.com

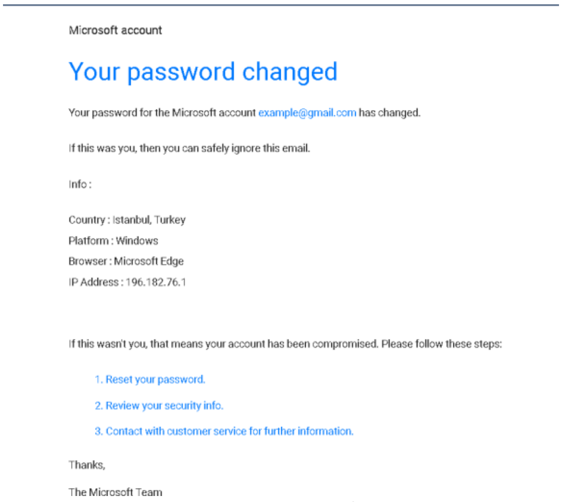
Date
21.12.2023 16:02:15

Password
123456

Selected Page
Netflix

IP Address
111.111.1.1

Fig. 5. Administration Page



Microsoft account

Your password changed

Your password for the Microsoft account example@gmail.com has changed.

If this was you, then you can safely ignore this email.

Info :

Country : Istanbul, Turkey
Platform : Windows
Browser : Microsoft Edge
IP Address : 196.182.76.1

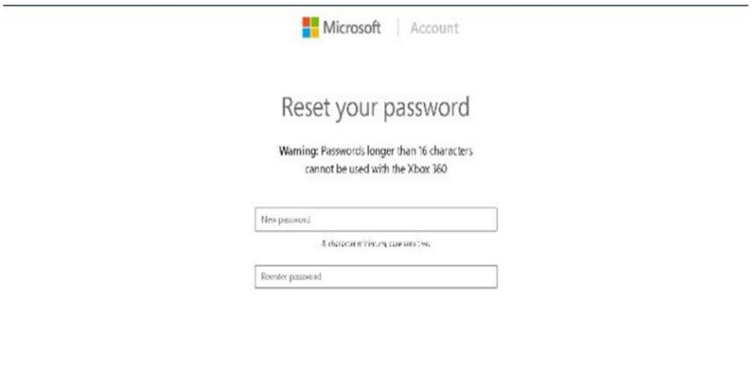
If this wasn't you, that means your account has been compromised. Please follow these steps:

1. Reset your password.
2. Review your security info.
3. Contact with customer service for further information.

Thanks,

The Microsoft Team

Fig. 6. Fake Microsoft E-mail



Reset your password

Warning: Passwords longer than 16 characters cannot be used with the Xbox 360

New password

8 characters minimum; case sensitive

Reenter password

Fig. 7. Fake Microsoft Web Page

REFERENCES

Alotaibi, M., Furnell, S. and Clarke, N., 2016, December. Information security policies: a review of challenges and influencing factors. In 2016 11th International Conference for Internet Technology and Secured Transactions pp. 352-358. IEEE.

P. Puhakainen and M. Siponen, "R ESEPJRCH A RTICLE I MPROVING E MPLOYEES ' C OMPLIANCE T HROUGH I NFORMATION S YSTEMS S ECURITY T RAINING :," 2010, vol. 34, no. 4, pp. 757-778.

J. D'Arcy, A. Hovav, and D. Galletta, "User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach," Inf. Syst. Res., vol. 20, no. I, pp. 79-98, 2009

2020 13th International Conference on Developments in eSystems Engineering (DeSE) | 978-1-6654-2238-3/20/$31.00 ©2020 IEEE | DOI: 10.1109/DeSE51703.2020.9450238

INTERNET REFERENCES

[1] https://perception-point.io/blog/how-to-conduct-a- phishing-attack-5-easy-steps/

[2] https://www.itgovernance.co.uk/phishinghttps://cdn.sparkfun.com/ assets/f/f/a/5/0/DS-16038.pdf

[3] https://www.techtarget.com/searchsecurity/definition/phishing

[4] https://www.cisco.com/c/dam/en_us/about/doing_business/trust- center/docs/phishing-program-infographic.pdf