

Social Engineering Attack: E-mail Phishing System

Tolga Emre Koraş
Emin Mert Demirci
Supervisor Prof. Dr. Emre Olca
Software Engineering
Maltepe University
İstanbul, Türkiye
200706042@st.maltepe.edu.tr
180706023@st.maltepe.edu.tr
emreolca@maltepe.edu.tr

Abstract- This project uses the E-mail phishing method, which is one of the social engineering attacks. The aim of the project is to observe and learn how E-mail phishing attacks, which are very popular today and still continue to increase in number, progress using the method, to create a little information among ordinary people and to speculate on how precautions can be taken with the information we have about these attacks. The system is designed in a simple and clear way that anyone can use and understand. The user sees firsthand how Phishing attacks work. The user enters the created WEB site, selects sample fake e-mail templates from the site's database, initiates an e-mail phishing attack and observes how it works.

Keywords— *Phishing attack, E-mail, database, WEB site, social engineering attacks.*

I. INTRODUCTION

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.

II. 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.

III. Social Engineering Attack: E-mail Phishing System

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.

The project consists of 3 parts. The parts are given below.

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.

IV. SYSTEM ARCHITECTURE

In this part of the documentation, there are diagrams and designs explaining the structure and operation of the project. Sequence diagram, activity diagram and flow chart of the project are given below.

Admin logs in to the system and sends an email to the target via the web application. The target clicks on the email and its information is transferred from the web application to the database. After the target clicks on the link in the email, the target is directed to the fake page. On this page, the necessary information is obtained from the target and this information is sent to the database. An error message is then given to the target. Admin can also obtain the information entered by the target by pulling it from the database through the application.

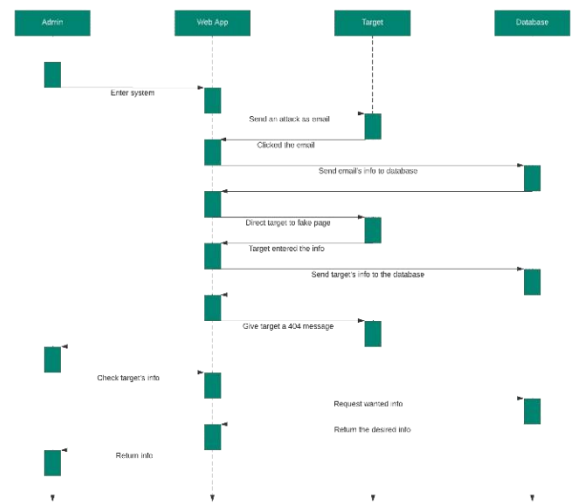


Fig. 1. The Sequence Diagram of Project

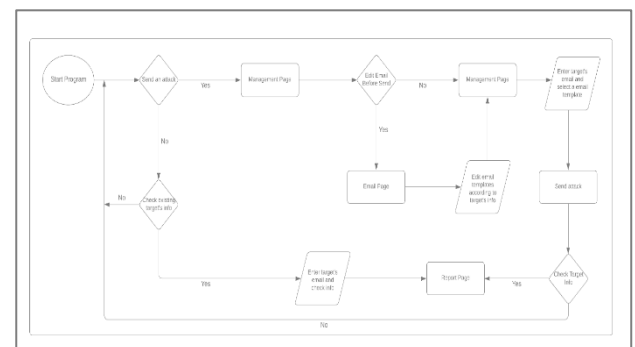


Fig. 2. The UML Activity Diagram of Project

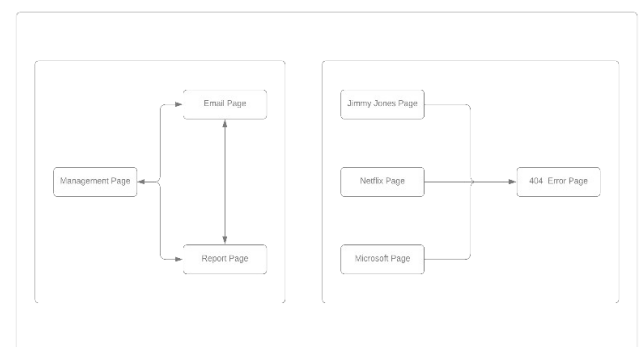
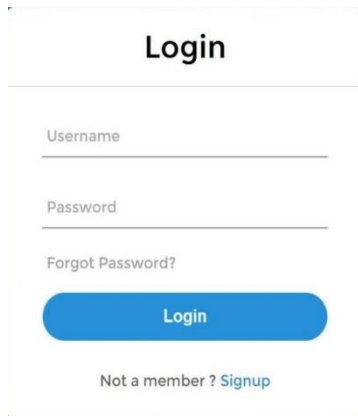


Fig. 3. Flow Chart of the Project

A. Web site

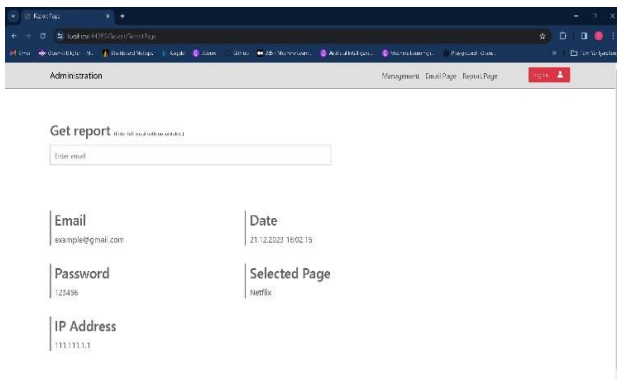
In this section, it shows how web site works, user enters the system.



The login page features a central heading "Login" in bold black text. Below it are two input fields: "Username" and "Password", each with a horizontal line for text entry. A link "Forgot Password?" is positioned below the password field. A prominent blue "Login" button is centered below the fields. At the bottom, a link "Not a member ? Signup" is displayed in blue text.

Fig. 4. Log-in Page

admin control the system via using Pages. It also shows (on the right) how the target uses the system via using fake web pages made by us.

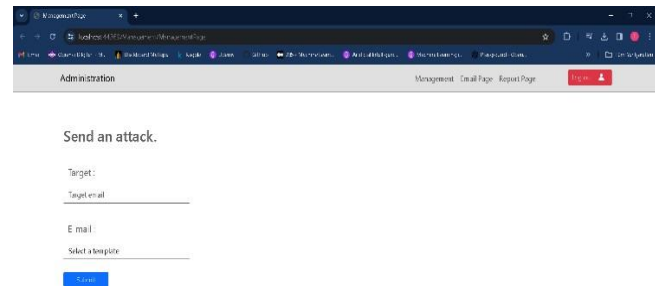


The administration page has a top navigation bar with links: "Administration", "Management", "Email Page", and "Report Page". The main content area includes a "Get report" section with a text input field labeled "Enter email". Below this is a table with two columns: "Email" and "Date". The table contains one row with the email "example@gmail.com" and the date "21/12/2022 18:02:15". Another section shows fields for "Password" (value: "123456") and "Selected Page" (value: "Netflix"). At the bottom, the "IP Address" is listed as "111.111.1.1".

Fig. 5. Administration Page

The application is started. If an attack is wanted, it goes to the admin management page. From here, the user can send an e-mail to the target by entering the target's information and the template information he wants to use, or send the document he edited by editing it according to the target before sending the e-mail. After performing the attack, the admin can go to the report page to view the information from the user. If not, the procedures described above are applied to send a new attack. In addition, if the admin does not want to attack in the first place (in case an attack has already been made), he can check and view the information of previous attacks by entering the report page.

Our application contains 3 pages for admin and 4 pages for target user. Of course, target user can't access the admin's pages.

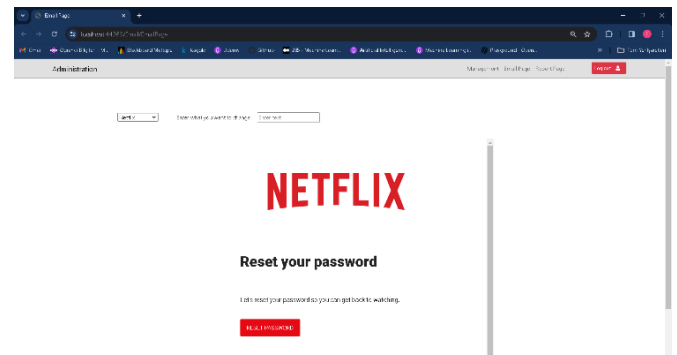


The management page is titled "Send an attack." and includes a "Target:" section with a "Target email" input field. Below this is an "Email" section with a "Select a template" dropdown menu and a blue "Send" button.

Fig. 6. Management Page

In Figure 6, admin can send a phishing attack to the target user via this page. Admin enters target user's information and selects a template according to target user.

Admin can navigate between pages and enter these pages and perform the necessary actions from there. The target user is directed to the pages shown in the flow chart from the link he clicked in the email (Fig.8.), enters the necessary information here and presses the send button. After pressing the button, an error message screen appears to the target user. Admin can review the target user's information from the report page. Admin can review email templates from the email page and change these templates according to the target user. On the management page, the admin organizes a phishing attack by selecting the email address of the target user and the template he wants to send.



The email template page displays a "NETFLIX" logo in red. Below it, the text "Reset your password" is shown, followed by a message: "Let's reset your password so you can get back to watching." A red "Reset Password" button is located at the bottom of the form.

Fig. 7. Email Template Page

In figure 7, the admin can change the content of the email templates by arranging the previously created email templates according to the target user. In this way, the prepared template is prepared specifically for the target users and reduces the user's suspicion.

In figure 5, the admin can view the information entered by the target user on the report page. Admin can also see the information of other target users from here. Information about the desired target user is displayed from the search bar on this page.

NETFLIX

Reset your password

Hi Tolga,

Let's reset your password so you can get back to watching.

RESET PASSWORD

If you did not ask to reset password, [click here](#) to login and reset your password immediately to avoid unauthorized activity on your account.

We're here to help if you need it. Visit the [Help Center](#) for more info or just [contact us](#).

The Netflix Team

Fig. 8. Send E-mail

Fig. 9. Fake Netflix Page

Figure 9 is the fake Netflix webpage where target user enters his/her information to enter the system. After target user enters information, we get the info of target.

Fig. 10. Fake Microsoft E-mail

Figure 9 is the email page of Microsoft. In this page target user should click 1.reset your password link to access our fake website of Microsoft.

Fig 11. Fake Microsoft Web Page

Figure 11 is the fake webpage of the Microsoft where target user enters his/her information, after target user click Next button, we get the target user's information.

Fig. 12. Fake Jimmy Jones E-mail

Figure 12 is email page of the Jimmy Jones. User should again click the button which says 'ORDER NOW' to direct to the fake webpage.

B. Database

In this section, the database entities used by the system, its design and relationships are included. Figure 13 represents the ER model of the database of the system.

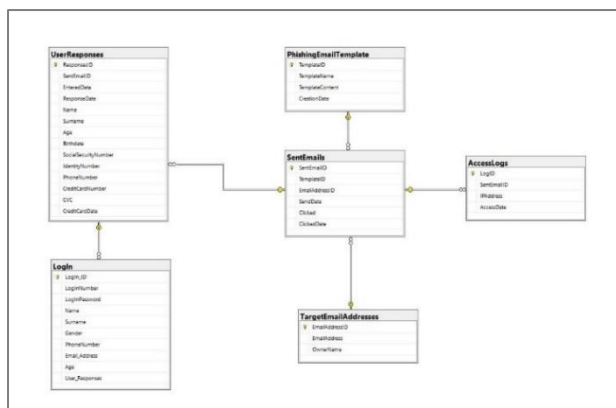


Fig. 13. ER Database Model

V. 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.

REFERENCES

- [1] 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.
- [2] P. Puhakainen and M. Siponen, "R ESEPTJRCH 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.
- [3] 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. 1, pp. 79-98, 2009.
- [4] <https://perception-point.io/blog/how-to-conduct-a-phishing-attack-5-easy-steps/>
- [5] <https://www.itgovernance.co.uk/phishinghttps://cdn.sparkfun.com/assets/f/f/a/5/0/DS-16038.pdf>
- [6] <https://www.techtarget.com/searchsecurity/definition/phishing>
- [7] https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/phishing-program-infographic.pdf
- [8] 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

- [9] P. Bhardwaj, A., Sapra, V., Kumar, A., Kumar, N. and Arthi, S., 2020. Why is phishing still successful? Computer Fraud & Security, 2020(9), pp.15-19
- [10] <https://www.ibm.com/topics/phishing>