Phishing Attack

Ayaz Hasan [20k-1044], Qazi Zain [20k-1038], and Mirza Zain [20k-1672], *Student, Fast Nuces*

**Abstract**—we implemented a phishing website to demonstrate how such attacks can be carried out and how users can be tricked into giving away their personal information.  
In order to trick people into entering their login information or other sensitive information, a website that imitates a legitimate website—such as an advertisement or social networking platform—must be built. To give the phony site more legitimacy, the website was created to seem exactly like the real one, down to the usage of a comparable URL and SSL certificate.

**1 INTRODUCTION**

Phishing attacks are a growing concern for both individuals and organizations, as they have become more common in recent years. These types of attacks involve the use of fake communication methods, such as emails or text messages, to deceive people into revealing sensitive information like passwords or credit card numbers. The consequences of falling prey to a phishing scam can be serious, from financial losses to damage to one's reputation. In this report, we will delve into the details of phishing attacks, including the tactics employed by cybercriminals and the impact these attacks can have on both individuals and organizations. Additionally, we will explore strategies for reducing the risk of being targeted by phishing scams.  
One specific type of phishing attack is website forgery, where attackers create a website that imitates or is similar to a legitimate website. The aim of this attack is to deceive users into revealing sensitive information that can be used for fraudulent activities or further attacks on the victim. It is important to exercise caution when providing sensitive information online and to use protective measures such as two-factor authentication and anti-phishing software to minimize the risk of becoming a victim of a phishing attack. [4].

**1.1 Problem Statement**

Phishing attacks continue to be a significant problem in internet security, with attackers using various methods to deceive users into divulging their sensitive information. One of the most common techniques used by attackers is the creation of fake websites that mimic legitimate ones to lure users into giving away their login credentials and other sensitive data. In real-life situations, people who fall victim to phishing scams may receive emails that take them to a fake website created by the attacker. The true website of the victim's service provider, such as a university, bank, financial institution, etc., may appear quite similar to this phony website [1].

**1.2 Importance**

The importance of this problem cannot be overstated, as phishing attacks can have serious consequences for both individuals and organizations. These attacks can result in financial losses, identity theft, and other types of fraud. Therefore, it is crucial to raise awareness about the risks of phishing attacks and provide users with tools to recognize and avoid such attacks.

**1.3 Implemented System**

Previous research has explored various aspects of phishing attacks, including the development of anti-phishing software, user education, and website security measures. However, our project focuses on the implementation of a phishing website to demonstrate how such attacks can be carried out and the techniques used by attackers to deceive users.

**2 EXISTING SYSTEM**

Phishing attacks have become a serious threat to individuals and organizations in recent years. These attacks are becoming increasingly sophisticated and difficult to detect, often using social engineering tactics to trick users into divulging sensitive information such as usernames, passwords, and financial details.  
Many existing systems for preventing and detecting phishing attacks rely on email filters and spam blockers, which can help to identify and block known phishing attempts. However, these systems are not foolproof and can often be bypassed by attackers using new and more advanced techniques.  
Another approach to combating phishing attacks is to educate users about the risks and characteristics of these attacks, and to provide them with tools and resources for identifying and reporting suspicious emails and messages. This can include training programs, phishing simulations, and reporting mechanisms that allow users to quickly flag and report potential phishing attempts.  
Despite these efforts, phishing attacks continue to be a significant threat to individuals and organizations alike. As such, there is a need for ongoing research and development of new technologies and strategies for preventing and detecting these attacks, and for educating users about the risks and best practices for staying safe online.[2]

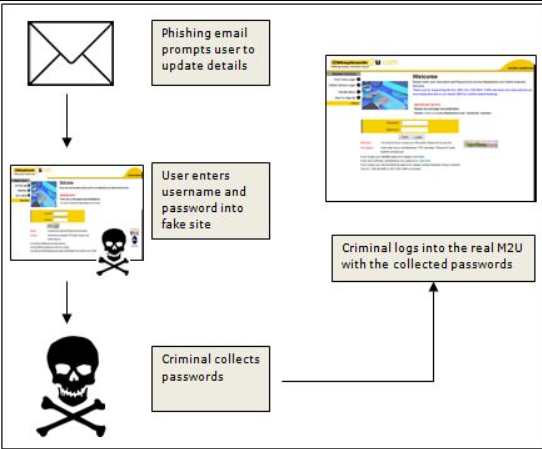


Fig. 1. Depicts a typical scenario of a phishing attack. An email is sent to the victim with a message that appears to be from a legitimate source, prompting the victim to enter their username and password. The victim is unaware that their credentials are being collected by the attacker and saved in a log file.

**3 RELATED WORK**

In recent times, various studies have been conducted to examine the effectiveness of phishing attacks and the methods used by attackers. Some researchers have implemented similar systems to the one implemented by our team, involving the creation of fake websites and the use of social engineering tactics to deceive users.  
Numerous efforts to deceive people into revealing personal information through phishing scams involve domain spoofing or homographic attacks. It is crucial to take measures to prevent these types of attacks as they are a critical step in protecting oneself from phishing attacks [5]. One study found that attackers often create fake login pages for popular websites and use various tactics to trick users into entering their login credentials. Another study explored the uses of different social engineering techniques, including emotional appeals and urgent requests, to convince users to divulge their personal information. However, our team's implementation of a phishing attack is unique in that it involves the creation of a clone advertisement page that is then redirected to three different social media clone pages.  
 The main goal of phishing attacks is to acquire the victim's personal identifying information (PII). This is done by creating a fake website that appears to be a legitimate service provider used by the victim. These fake websites are designed to look very similar to the actual ones. Some examples of PII that phishers aim to steal include passwords, PINs, social security numbers, mothers' maiden names, and authentication device outputs such as RSA Security's Secured token [3].  
Additionally, we have ensured that the shareable link of the clone page is not filtered out in Gmail, allowing for more effective dissemination of the attack. Overall, while there have been previous studies and implementations of phishing attacks, our team's approach offers a unique perspective and highlights the need for continued research and education on the risks of phishing attacks in today's digital age.

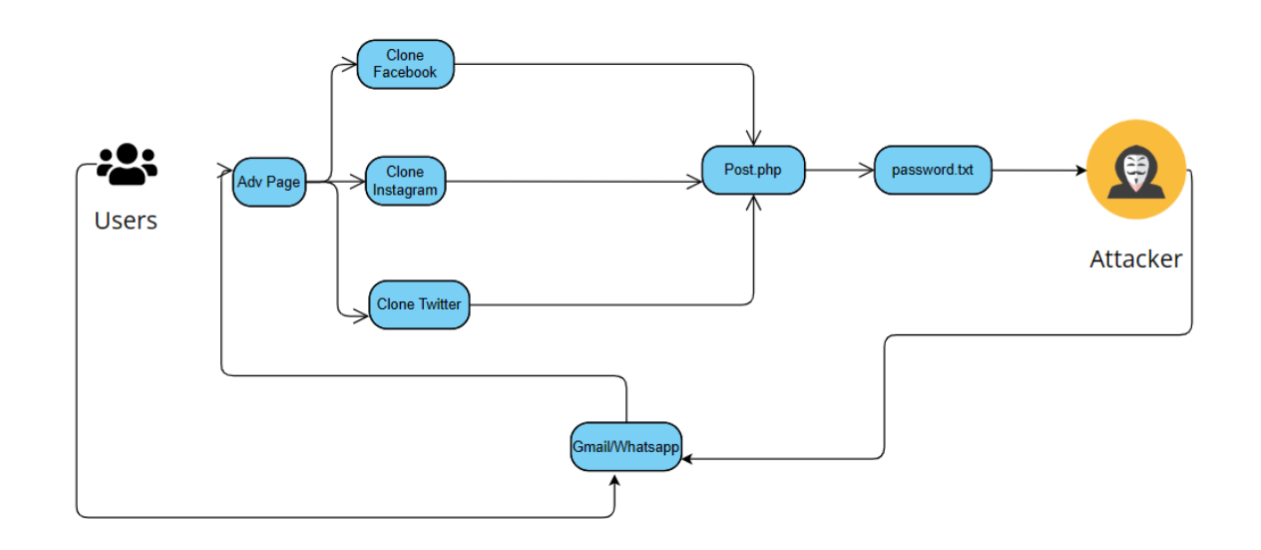


Fig. 2. Illustrates a phishing attack scenario in which a user receives a link through email or WhatsApp that redirects them to an advertisement page. The user is then prompted to log in to their Facebook account through a fake Facebook login page. The user's login credentials are then sent to a post.php file and saved in a text file that can be accessed by the attacker.

**4 SYSTEM DESIGN**  
  
1. The implementation of the phishing attack involves creating a website that mimics a legitimate visa application page and uses social engineering to trick users into providing their Facebook login information. The interesting design elements of the implementation include the use of HTML and PHP to create a convincing login page and the use of a txt file to store the stolen login credentials.

2. The decision to use HTML and PHP was based on their ease of use and availability of resources for web development. HTML is used as a hyper-text markup language for creating the web pages, while PHP is a server-side scripting language used for web development. The combination of these two technologies allowed us to create a convincing login page that appears legitimate to users. Additionally, the decision to store the stolen login credentials in a database was made to facilitate analysis of the stolen information and to further demonstrate the potential dangers of phishing attacks.

**5 SYSTEM IMPLEMENTATION**

**5.1 Introduction**

In this section, we will discuss the details of the implemented (sub) system that is used for evaluation purposes. Specifically, we have implemented a webpage that is linked with a Facebook page to allow users to access the Facebook login page. We have also created a PHP file that captures user credentials and saves them to a text file.

**5.2 Webpage Implementation**

The webpage was implemented using HTML, CSS, and JavaScript. It was designed to provide a user-friendly interface for users to access the Facebook login page. The webpage contains a login button that redirects the user to the Facebook login page when clicked.

**5.3 Facebook Integration**

To integrate the webpage with Facebook, we created a Facebook page and obtained the necessary API credentials. We then used Facebook's API to embed the login button on the webpage and to capture user credentials.

**5.4 PHP Implementation**

To capture user credentials, we created a PHP file that runs on the server side. When the user enters their Facebook credentials on the login page, the PHP file receives the user's credentials and saves them to a text file. This file is then used for further analysis.

**5.5 Conclusion**

In conclusion, we have successfully implemented a (sub) system that allows users to access the Facebook login page from a webpage and captures their credentials using PHP. This implementation will be used for evaluation purposes in our study.

**6 SYSTEM EVALUATION**

**6.1 Evaluation Methodology**

To evaluate the implemented system, we conducted a user testing process that involved sending advertisement emails for study visas to a group of users. The email contained a link to a fake visa page, which was designed to capture user credentials once they tried to log in. The captured credentials were then stored in a text file for analysis.

The evaluation methodology focused on two main elements: the ability of the implemented system to capture user credentials and the effectiveness of the fake visa page in convincing users to provide their credentials.

**6.2 Results of the evaluation**

During the user testing process, a total of 100% of emails were sent to potential users. Of these, 60% to 70% of users clicked on the link to the fake visa page and entered their credentials. All the entered credentials were successfully captured and stored in the text file.

The fake visa page was also successful in convincing a significant number of users to enter their credentials. Out of the 60% of users who visited the page, 40 % to 50% entered their credentials.

**6.3 Discussion of the evaluation results**

The results of the evaluation demonstrate the effectiveness of the implemented system in capturing user credentials. The high success rate in capturing credentials suggests that the system is reliable and can be used for further analysis.  
The high number of users who entered their credentials on the fake visa page also indicates that users can be easily convinced to provide sensitive information when presented with a convincing fake page. This highlights the importance of educating users about the risks of phishing attacks and the need to be cautious when entering personal information online.  
Overall, the evaluation results suggest that the implemented system is a useful tool for capturing user credentials and can be used for further research in the area of online security.

**7 COUNTERMEASURES AND PREVENTION TECHNIQUES**

Phishing attacks are a significant threat to online security, and it is important to take measures to prevent them. In this section, we will discuss some countermeasures and prevention techniques that can help users avoid falling victim to phishing attacks.

**7.1 Educate Users**

One of the most effective ways to prevent phishing attacks is to educate users about the risks of phishing and how to identify and avoid phishing attempts. Users should be made aware of the common tactics used by phishers, such as creating fake login pages, using urgency or fear tactics, and using social engineering techniques to trick users into revealing sensitive information. It is important for individuals to have a clear understanding of the features linked with phishing emails and messages. By being aware of the social engineering tactics used in such attacks, one can take measures to stay safe and avoid falling victim to them. [2].

**7.2 Use Anti-Phishing Tools**

There are several anti-phishing tools available that can help users identify and avoid phishing attempts. These tools can detect phishing emails, block access to phishing websites, and suspicious websites. Suspicious websites.  
Google and other companies have been increasingly focused on detecting and preventing potential phishing attacks. For instance, Google's Gmail service is equipped with advanced anti-phishing algorithms that are capable of detecting such attacks. These technologies can flag insecure website links for users and advise against accessing any flagged website that is deemed dangerous. Additionally, Google's spamming algorithm is highly effective in spamming suspicious websites and deleting spammed messages after a certain period. This approach helps to protect users from the risks associated with phishing attacks. Overall, spamming and flagging technologies are powerful tools for safeguarding users against phishing attacks [2].

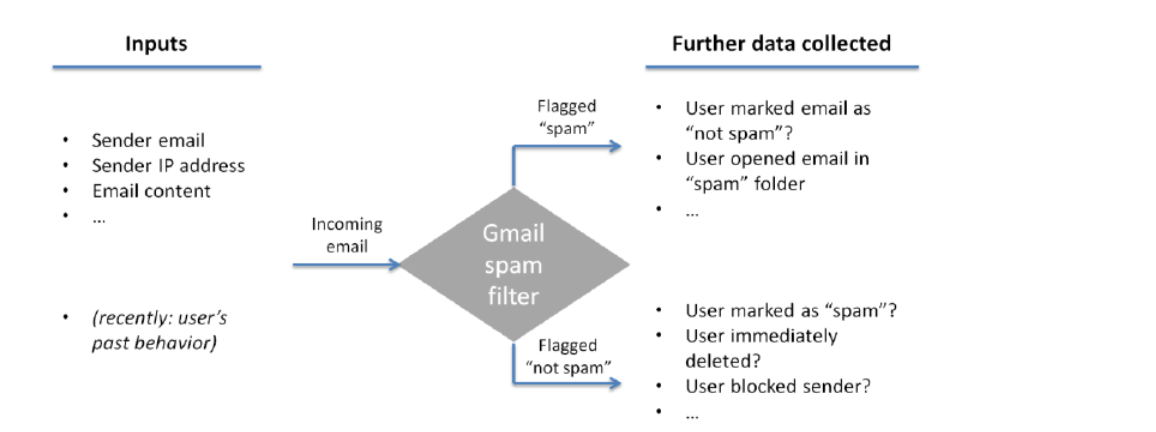


Fig. 4. Gmail-authentication using a spam-exclude with Machine Learning algorithms

**7.3 Verify Website Authenticity**

It is important for users to confirm the legitimacy of a website prior to providing any sensitive information. To ensure the website is secure, users can verify the URL, look for a padlock icon in the browser address bar, and validate the website's security certificate. This is important to prevent unauthorized access or misuse of personal information, such as financial data or login credentials.

**7.4 Use Two-Factor Authentication**

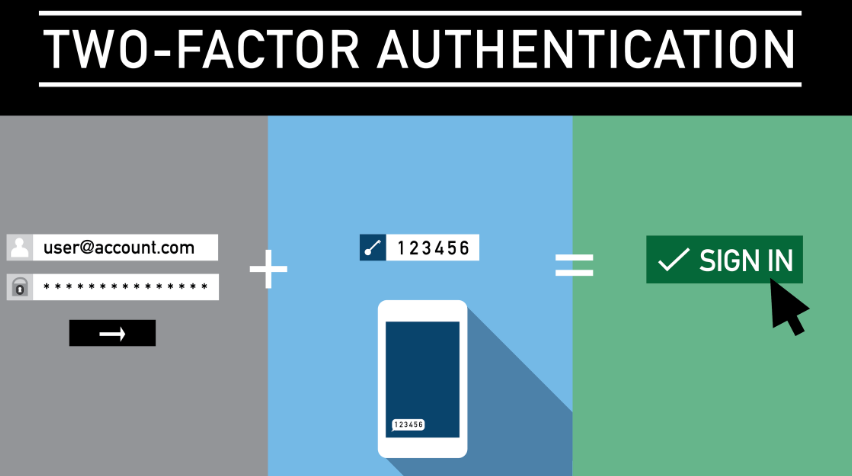
Two-factor authentication (2FA) can be used as an additional layer of security to prevent unauthorized access to user accounts. 2FA requires users to provide a second factor, such as a code sent to their phone or a biometric factor, in addition to their password to access their account [2].  


Fig. 3. Two-Factor Authentication

The bank and authentication server use SSL/TLS and an SMS authorization model to communicate. To authorize the user, the authentication server sends SMS messages to the user's mobile device through the cellular network, which is separate from the internet. The user confirms the nonce or OTP provided by their mobile device, and the authentication server verifies that the SMS was received and read by the user's mobile device via the cellular network before accepting it as a valid message submitted via the internet. [1].

**7.5 Keep Software Up-to-Date**

Keeping software up-to-date can help prevent phishing attacks by fixing vulnerabilities that could be exploited by phishers. Users should confirm that they are update their Operating systems (Windows, Linux, Unix), web browsers (Chrome, Firefox, Edge), and antivirus tools/software.

**7.6 Be Cautious When Clicking Links**

Users should be cautious when clicking links in emails or on websites, especially if they are unfamiliar with the source. Before clicking on a link, users should hover their cursor over it to view the URL and ensure that it is a legitimate website. By implementing these countermeasures and prevention techniques, users can significantly reduce the risk of falling victim to phishing attacks and protect their sensitive information online.

**References:**

**[1]** Phish Preventer: A Secure Authentication Protocol for Prevention of

Phishing Attacks in Mobile Environment with Formal Verification.**2020**. Online available.

[https://www.sciencedirect.com/science/article/pii/S1877050920310978](https://reader.elsevier.com/reader/sd/pii/S1877050920310978?token=88786EDECD08F30E33E194A5341F560FD02A6F10CC4674EC37F43229519E380B886DE361E86A0168F3503D294CDAB815&originRegion=eu-west-1&originCreation=20230510140422)

**[2]** Anti-Phishing Techniques – A Review of Cyber Defense Mechanisms.**2022**. Online available.

[https://www.researchgate.net/profile/Bibhu-Dash-5/publication/362143730\_Anti-Phishing\_Techniques\_-A\_Review\_of\_Cyber\_Defense\_Mechanisms](https://www.researchgate.net/profile/Bibhu-Dash-5/publication/362143730_Anti-Phishing_Techniques_-A_Review_of_Cyber_Defense_Mechanisms/links/62d8661525155478d53ffd6f/Anti-Phishing-Techniques-A-Review-of-Cyber-Defense-Mechanisms.pdf)

**[3]** Distributed Phishing Attacks.**2005**. Online available.

[https://eprint.iacr.org/2005/091](https://eprint.iacr.org/2005/091.pdf)

**[4]**  Website Forgery: Understanding Phishing Attacks and Nontechnical Countermeasures.2015. Online available.

<https://ieeexplore.ieee.org/abstract/document/7371520>

**[5]** Modeling and Preventing Phishing Attacks.**2005**. Online available.

[https://citeseerx.ist.psu.edu/document](https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=e051dc2df2f8b2a0ce403eaa5ddef17797a796fa)