Simulating an Internal Phishing Attack Using the Zphisher Tool

Date: 27.4.2025

By: Shuaib Salami

Overview

This project showcases the simulation of a phishing attack utilizing the Zphisher tool on Kali Linux. The demonstration involves crafting a replica of a legitimate login page from a well-known website, designed to capture user credentials upon a login attempt. This exercise is ***strictly for educational and ethical cybersecurity training purposes. It is important to note that conducting unauthorized phishing attacks is both illegal and unethical.***

Always obtain proper authorization before conducting any form of penetration testing.

Tools Used

- **Zphisher**: An automated phishing tool that supports various platforms.
- **Kali Linux**: A Debian-based Linux distribution used for penetration testing and security research.

- **Ngrok/Serveo**: Services to expose the phishing page to the internet.
-

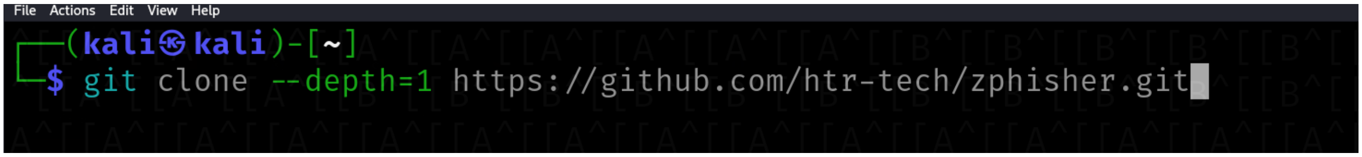
Installation

Prerequisites

- Kali Linux installed on your machine.
- Git installed on Kali Linux.

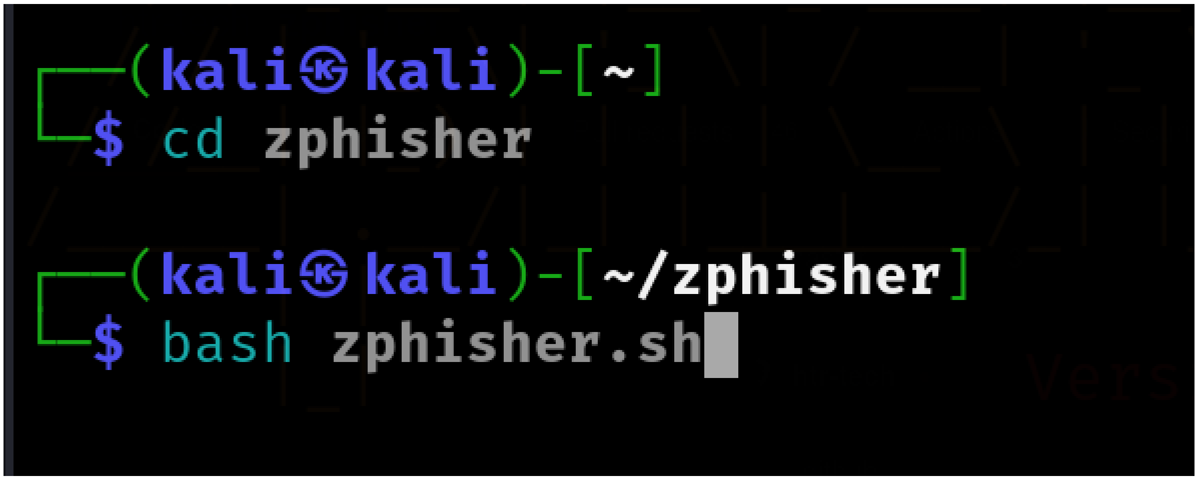
Steps to Install Zphisher

1. **Update your system**: sudo apt-get update & sudo apt-get upgrade to upgrade
2. **Clone the Zphisher**: Run the git clone git clone --depth=1 on kali



```
┌──(kali㉿kali)-[~]
└─$ git clone --depth=1 https://github.com/htr-tech/zphisher.git
```

3. Navigate to the Zphisher directory: cd zphisher
4. Give execution permissions: bash +x zphisher.sh



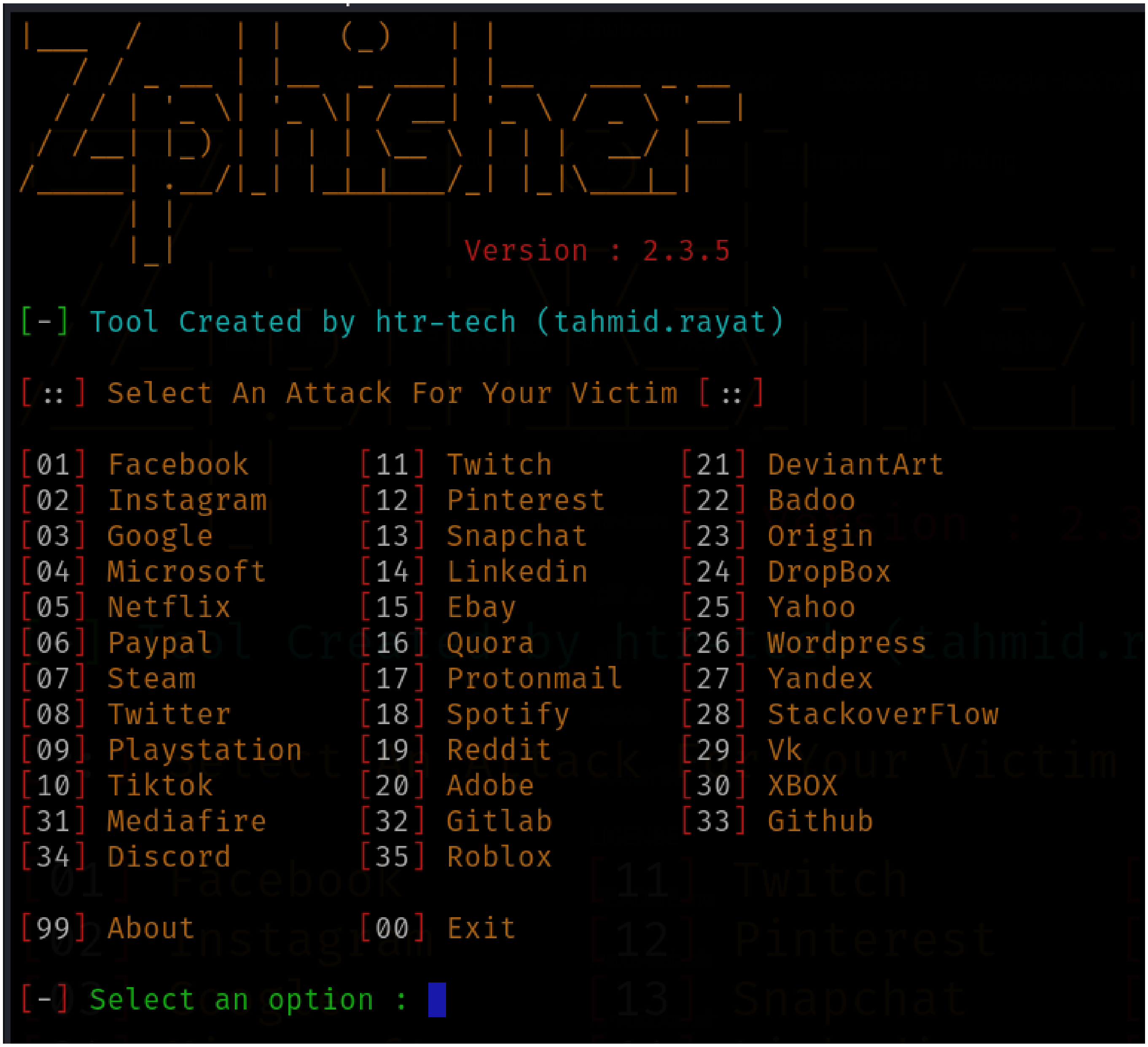
```
┌──(kali㉿kali)-[~]
└─$ cd zphisher

┌──(kali㉿kali)-[~/zphisher]
└─$ bash zphisher.sh
```

Then Give Execution permision: bash zphisher.sh

How to Perform the Phishing Attack

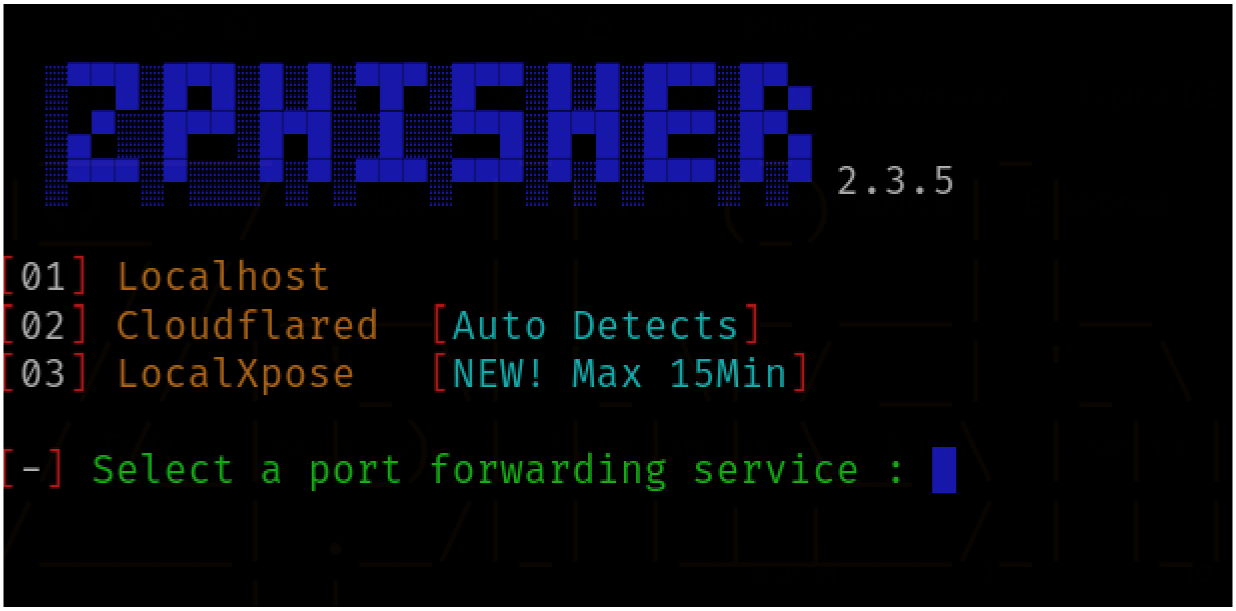
Step 1: Run Zphisher

1. **Start Zphisher**: ./zphisher.sh
2. **Select the phishing attack template** (e.g., Facebook, Instagram, Google).
3. **Choose the attack method** (Ngrok is recommended for easy public sharing).



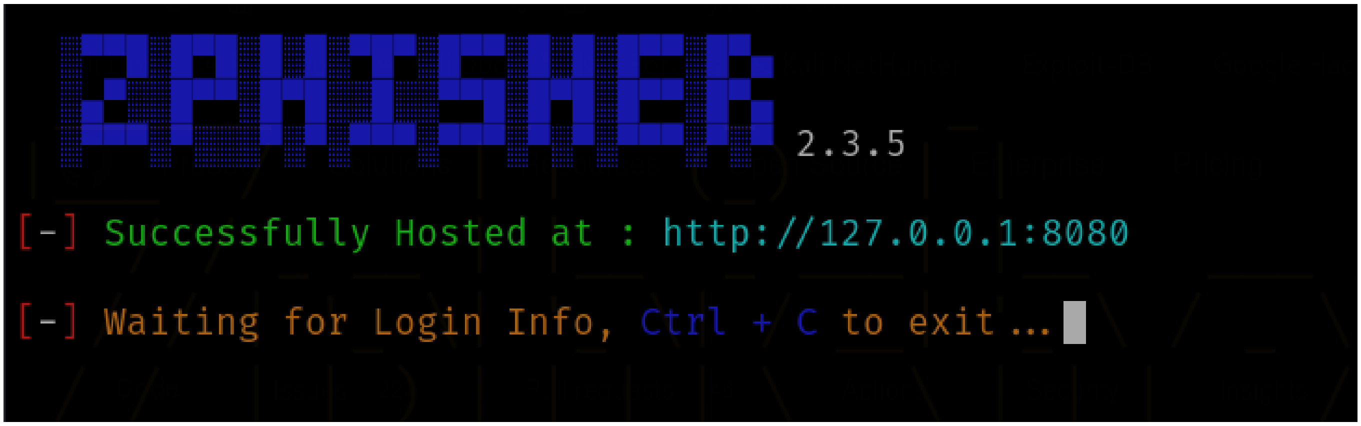
```
|___  /     | |   (_)   | |
   / / _ __ | |__  _ ___| |__   ___ _ __
  / / | '_ \| '_ \| / __| '_ \ / _ \ '__|
 / /__| |_) | | | | \__ \ | | |  __/ |
/_____| .__/|_| |_|_|___/_| |_|\___|_|
      | |
      |_|                Version : 2.3.5

[-] 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 :
```

Step 2: Customize the Phishing Page (Optional)



```
                                        2.3.5

[01] Localhost
[02] Cloudflared   [Auto Detects]
[03] LocalXpose    [NEW! Max 15Min]

[-] Select a port forwarding service :
```

1. **Edit the template** (Optional):
    a. Customize the HTML/CSS files in the sites directory to make the phishing page more convincing.
    b. Example: nano sites/yahoo/index.html



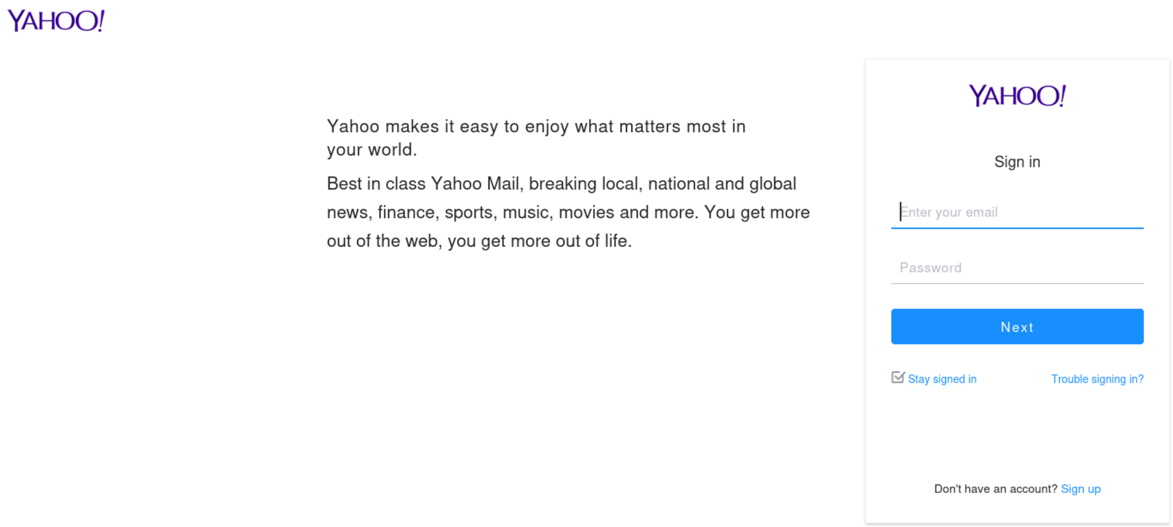
```
                                   2.3.5

[-] Successfully Hosted at : http://127.0.0.1:8080

[-] Waiting for Login Info, Ctrl + C to exit ...
```

Step 3: Deploy and Monitor

1. Copy the phishing URL generated by Ngrok or Serveo.

2. Share the phishing URL with the target user **(only with prior authorization and consent)**.

3. Monitor the Zphisher terminal for any login attempts and review the captured credentials in real-time.



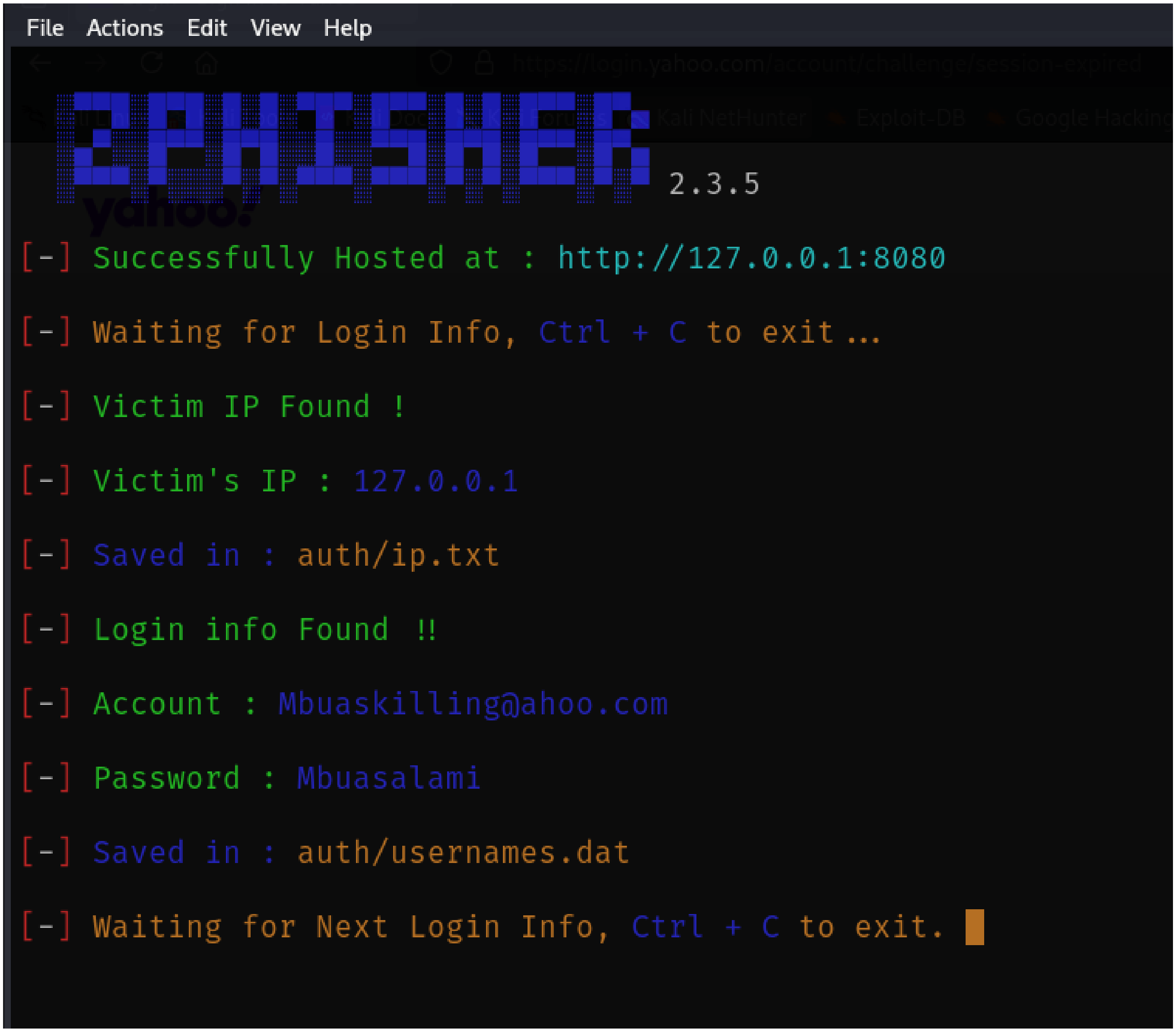
Yahoo makes it easy to enjoy what matters most in your world.

Best in class Yahoo Mail, breaking local, national and global news, finance, sports, music, movies and more. You get more out of the web, you get more out of life.

Step 4: Stop the Attack

1. **Terminate Zphisher**:

   a. Stop the attack by closing the terminal window or pressing CTRL + C. 2. **Analyze the captured data**.



```
2PHISHER 2.3.5

[-] Successfully Hosted at : http://127.0.0.1:8080

[-] Waiting for Login Info, Ctrl + C to exit ...

[-] Victim IP Found !

[-] Victim's IP : 127.0.0.1

[-] Saved in : auth/ip.txt

[-] Login info Found !!

[-] Account : Mbuaskilling@ahoo.com

[-] Password : Mbuasalami

[-] Saved in : auth/usernames.dat

[-] Waiting for Next Login Info, Ctrl + C to exit.
```

Ethical Considerations

- **Reflect on the Ethics**: Phishing is a serious security threat, and this knowledge should be used responsibly.
- **Report the Results**: If part of a security assessment, document your findings and provide recommendations to mitigate such attacks.

Disclaimer

This project is for educational purposes only. The author does not endorse or condone the use of this tool for illegal or unethical purposes. Use this information responsibly.

Recommendations:

- Enhance phishing awareness through ongoing, targeted training initiatives.
- Implement just-in-time educational interventions for users who engaged with phishing emails.
- Promote a proactive reporting culture by providing user-friendly reporting tools.
- Schedule regular follow-up phishing simulations to assess improvements and measure ongoing awareness.

Outcome:

The simulation successfully achieved its objectives by delivering valuable insights into employee responses and the organization's overall preparedness against phishing attacks. Moving forward, the findings will be integrated into continuous training programs and updated security policies to strengthen the organization's resilience against real-world cyber threats.

Conclusion

The phishing simulation effectively highlighted both the strengths and vulnerabilities in employee cybersecurity awareness. While the majority of users refrained from engaging with the phishing attempt, a significant portion clicked on malicious links or submitted credentials. This underscores the ongoing need for regular training and awareness programs to reinforce secure behavior and reduce susceptibility to social engineering attacks.

Report By: Salami Shuaib

Cybersecurity Analyst