Phishing Simulation Report

Cybersecurity Audit Project – Employee Vigilance Assessment

Organisation: Confidential

Date: Dec 22, 2025

Prepared By: Emmanuel Olajoseph
(Cybersecurity Analyst)

1 · Overview

A live phishing simulation measured employee vigilance against credential-harvesting attacks after a phishing-awareness training programme. The exercise focused on lowering link-click frequency, reducing credential submission attempts, and improving incident reporting.

2 · Objectives

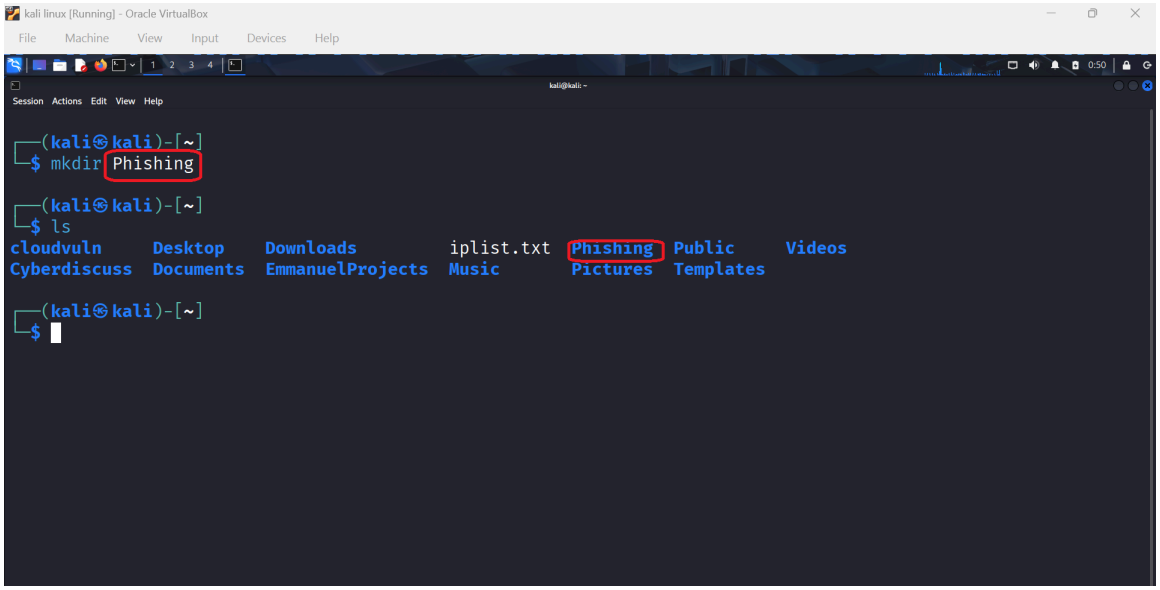
- Lower link-click rate among targeted employees.
- Increase phishing incident reports submitted to the security team.
- Reduce credential submission attempts on the phishing landing page.

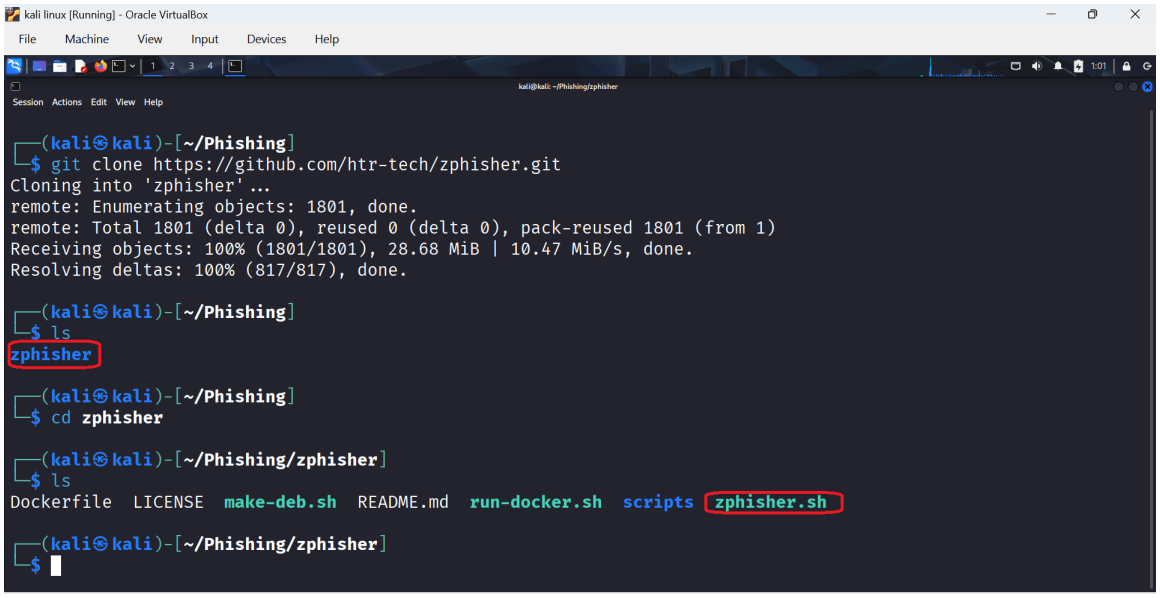
3 · Compliance Drivers

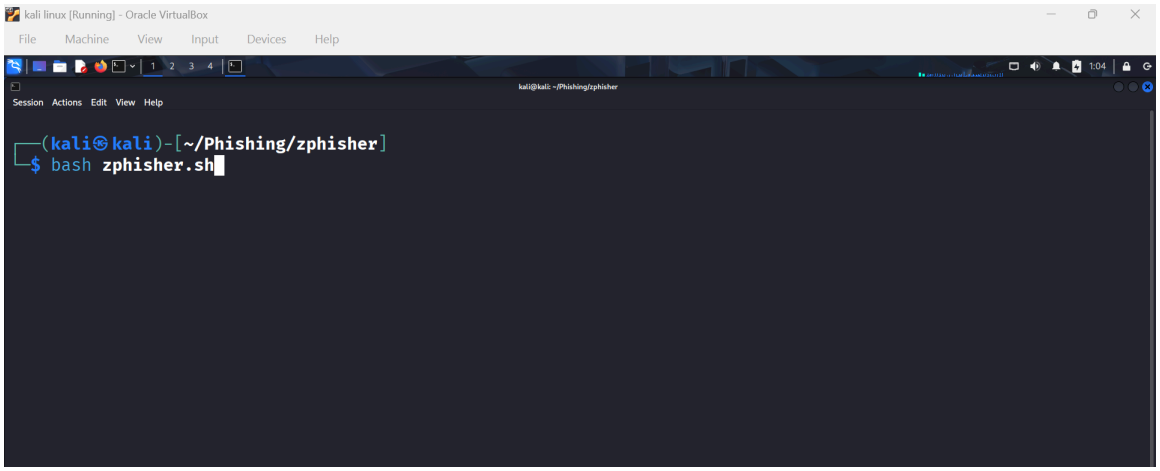
ISO/IEC 27001 user-awareness control (Annex A 6.3) demands measurable security education, while the internal risk register tracks progress against social-engineering risks.

4 · Tooling

- Zphisher – generated the phishing site and captured interaction data.
- Localxpose – optional port-forwarding for internal access during testing.
- Google Sheets – stored key performance indicators.

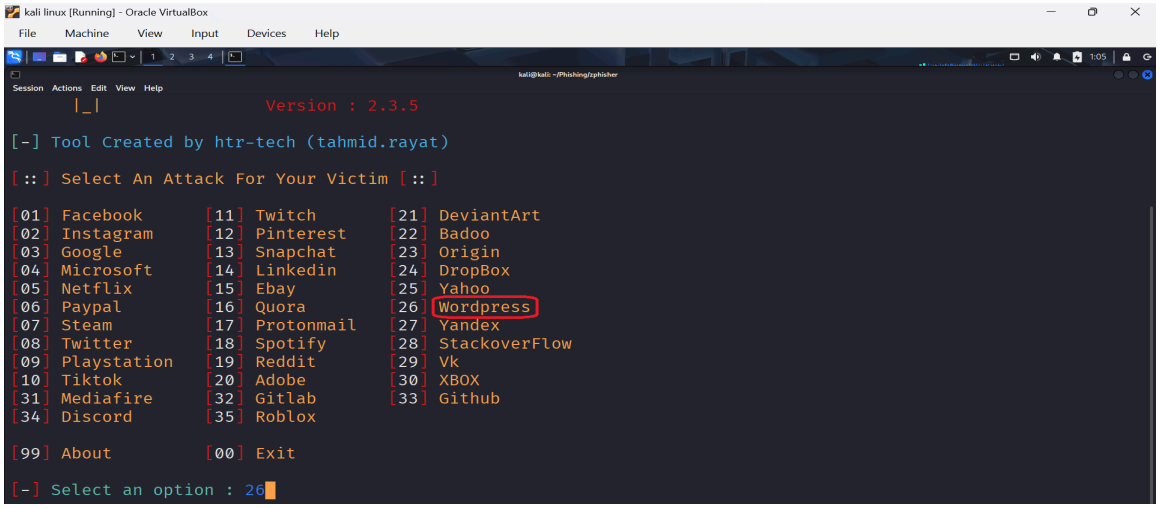


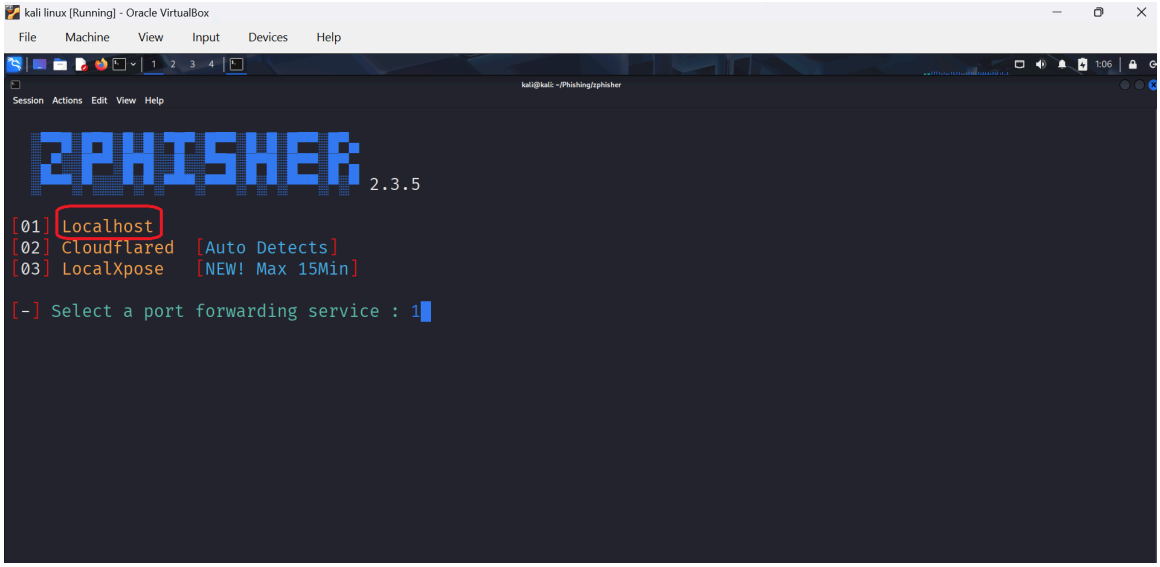

kali linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Session Actions Edit View Help
kali@kali: ~/Phishing/zphisher
┌──(kali㉿kali)-[~/Phishing]
└─$ git clone https://github.com/htr-tech/zphisher.git
Cloning into 'zphisher'...
remote: Enumerating objects: 1801, done.
remote: Total 1801 (delta 0), reused 0 (delta 0), pack-reused 1801 (from 1)
Receiving objects: 100% (1801/1801), 28.68 MiB | 10.47 MiB/s, done.
Resolving deltas: 100% (817/817), done.
┌──(kali㉿kali)-[~/Phishing]
└─$ ls
zphisher
┌──(kali㉿kali)-[~/Phishing]
└─$ cd zphisher
┌──(kali㉿kali)-[~/Phishing/zphisher]
└─$ ls
Dockerfile LICENSE make-deb.sh README.md run-docker.sh scripts zphisher.sh
┌──(kali㉿kali)-[~/Phishing/zphisher]
└─$

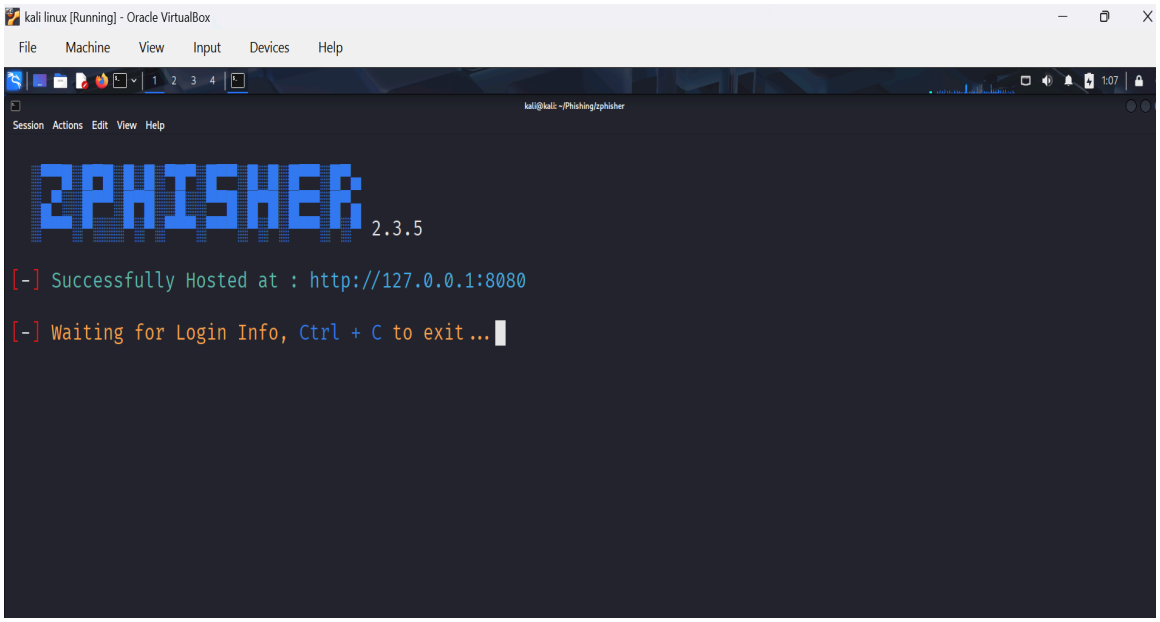

kali linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Session Actions Edit View Help
kali@kali: ~/Phishing/zphisher
┌──(kali㉿kali)-[~/Phishing/zphisher]
└─$ bash zphisher.sh

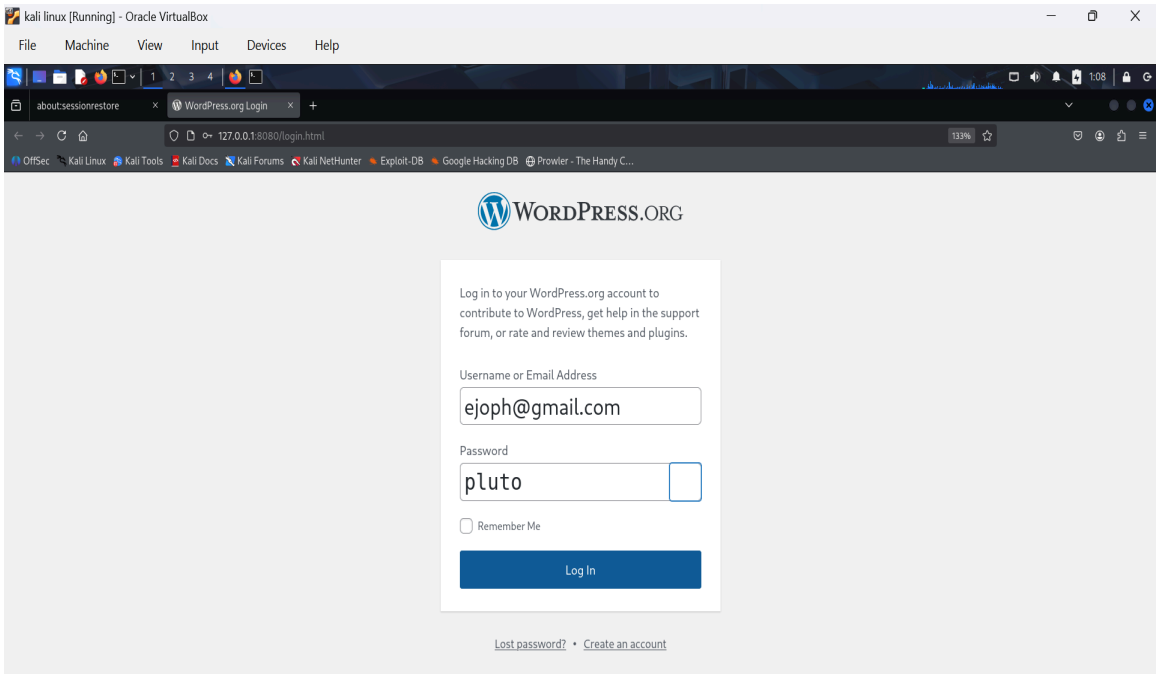
5 · Simulation Scenario

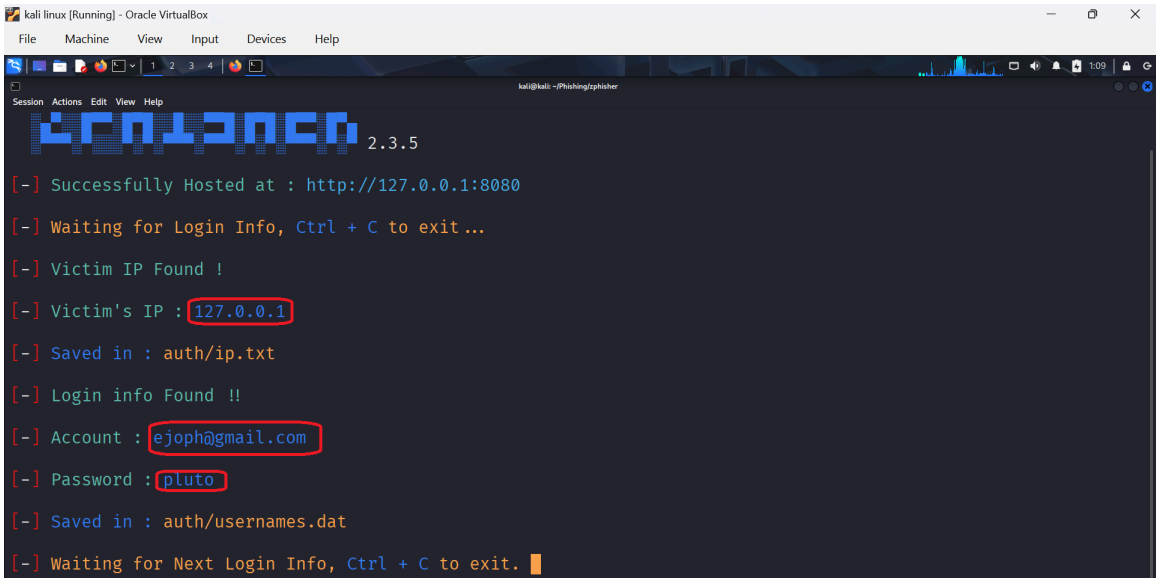
A crafted invoice-reminder email requested payment for WordPress services. The message included a link that directed recipients to a clone login page hosted with Zphisher.






kali linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Session Actions Edit View Help
kali@kali: ~/Phishing/zphisher
ZPHISHER 2.3.5
[-] Successfully Hosted at : http://127.0.0.1:8080
[-] Waiting for Login Info, Ctrl + C to exit...


kali linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
about:sessionrestore
WordPress.org Login
127.0.0.1:8080/login.html
WordPress.org
Log in to your WordPress.org account to contribute to WordPress, get help in the support forum, or rate and review themes and plugins.
Username or Email Address
ejoph@gmail.com
Password
pluto
Remember Me
Log In
Lost password? • Create an account



5.1 · Phishing Email Template

Hi Alex,

I hope this message finds you well. I am writing to remind you that the payment for the WordPress services provided on your domain cyberttech.com is now due. As per our agreement, the total amount of $4000 was to be settled by 29TH June, 2025.

We value our relationship and are committed to providing you with the best service possible. If you have already made the payment, please disregard this message. Otherwise, I kindly ask you to arrange for the payment at your earliest convenience.

Please click on this link if you have any questions or need further details regarding the invoice.

Thank you for your attention to this matter, and I look forward to continuing our successful collaboration.

Warm regards,

Wordpress team.

6 · Metrics

KPI	Baseline	Post-Campaign

Link clicks	80 %	30 %
Credential submissions	60 %	20 %
Phishing reports	10 %	80 %

7 · Analysis

- Link-click frequency fell by fifty percentage points, reflecting greater caution.
- Credential submission attempts dropped by forty percentage points, indicating stronger scepticism.
- The reporting rate rose by seventy percentage points, demonstrating proactive security behaviour.

8 · Recommendations

- Schedule quarterly phishing simulations to maintain awareness.
- Deliver refresher modules to employees who clicked or submitted credentials.
- Display live report metrics on the security dashboard for immediate visibility.
- Gamified Awareness Programs (leaderboards, recognition for reporting) to encourage higher vigilance.

9 · Conclusion

The simulation provided measurable evidence of improved employee vigilance. Results support ongoing investment in user-focused security controls and align with ISO 27001 requirements and risk-management goals.