Phishing Simulation Report

Cybersecurity Audit Project – Employee Vigilance Assessment

Organization: Confidential

Date: 12 December 2025

Prepared By: Temitope C Folowosele (Cybersecurity Analyst)

1 · Overview

A live phishing simulation evaluated employee vigilance against credential-harvesting attacks following a phishing-awareness training program. The exercise emphasized 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.

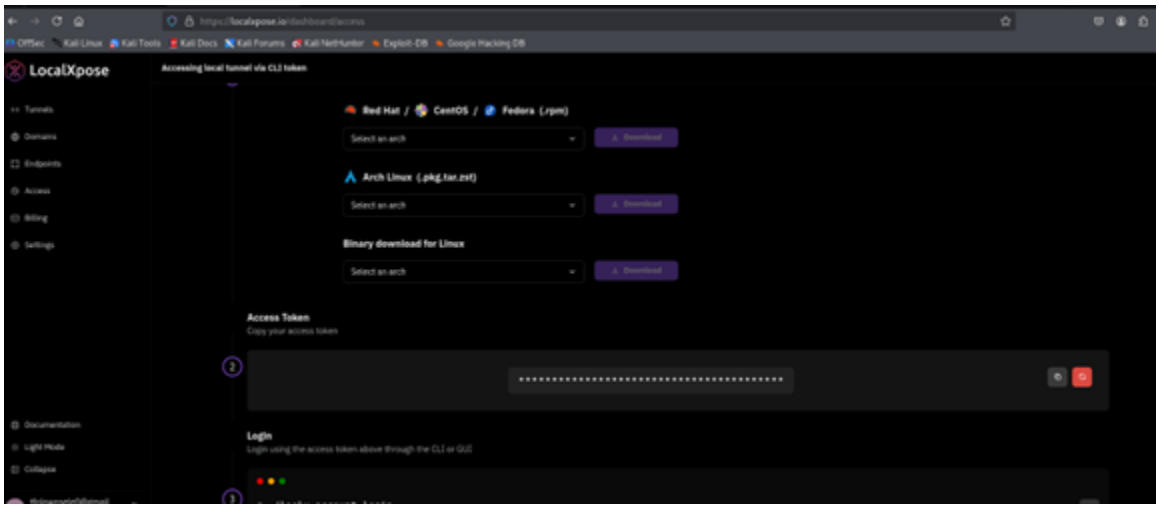
3 · Compliance Drivers

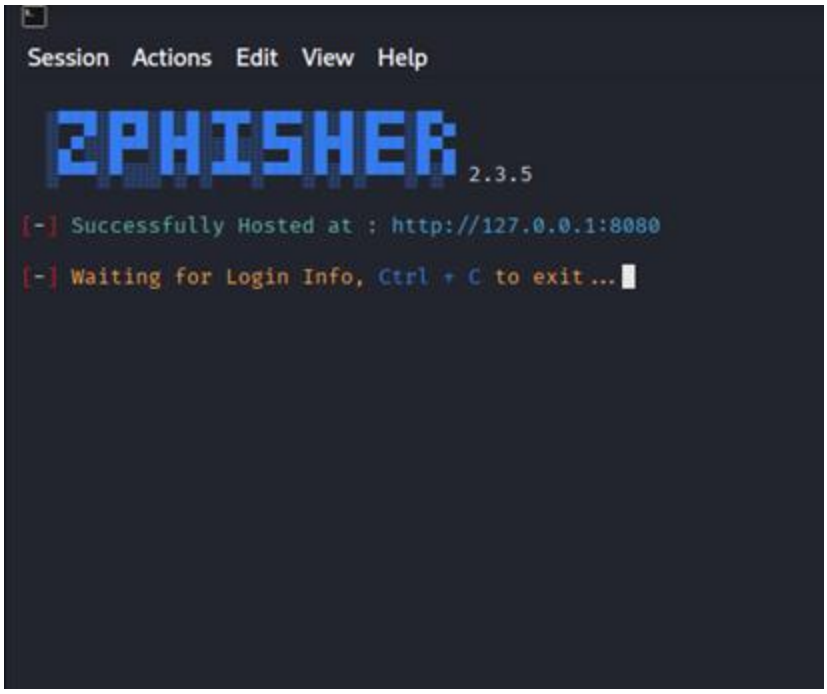
ISO/IEC 27001 user-awareness control (Annex A 6.3) demands measurable security education, while the internal risk register tracks progress against social-engineering risks.

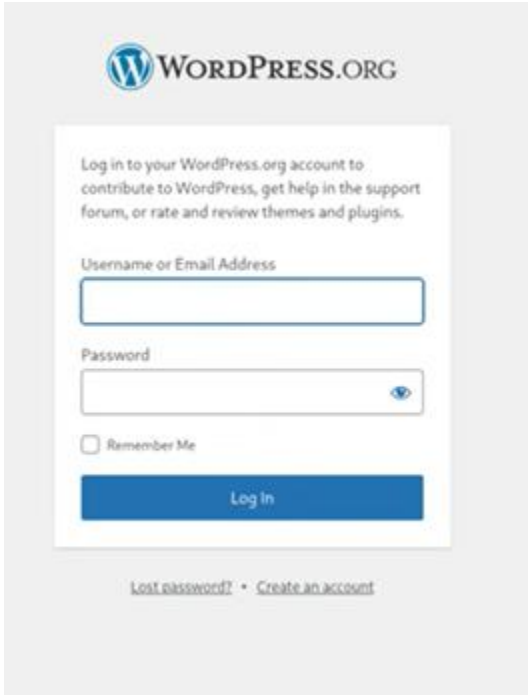
4 · Tooling

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


Session Actions Edit View Help
2PHISHER
2.3.5
[01] Localhost
[02] Cloudflared [Auto Detects]
[03] LocalXpose [NEW! Max 15Min]
[-] Select a port forwarding service :


LocalXpose
Accessing local tunnel via CLI token
Red Hat / CentOS / Fedora (.rpm)
Arch Linux (.pkg.tar.zst)
Binary download for Linux
Access Token
Login





5 · Simulation Scenario

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

5.1 · Phishing Email Template

Subject: ⚠️ Action Required: WordPress Payment Verification Needed

Hello Fred,

We detected an issue with your WordPress payment configuration that requires immediate attention.

Your most recent payment attempt could not be fully verified due to an account authentication error. To prevent service disruption, we require you to confirm your payment details.

Please click this link to review and verify your payment information:

If the issue is not resolved within 24 hours, your WordPress services (including plugins and themes) may be suspended.

Payment Details Summary: $2000

Platform: WordPress

Status: Pending Verification

Action Required: Immediate confirmation

If you believe this message was sent in error, please verify your account to ensure uninterrupted service.

Thank you for your prompt attention.

—

WordPress Billing Support

© WordPress.org

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 doubt.
- Reporting rate rose by seventy percentage points, demonstrating proactive security behavior.

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.

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.