

## **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.



The screenshot shows the Zphisher command-line interface. At the top, there's a navigation bar with 'Session', 'Actions', 'Edit', 'View', 'Help', and a power icon. Below the title 'ZPHISHER' and version 'Version : 2.3.5', it says '[-] Tool Created by htr-tech (tahmid.rayat)'. It then displays a menu with the instruction '[-] Select An Attack For Your Victim [-]'. The menu lists various platforms in three columns:

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		

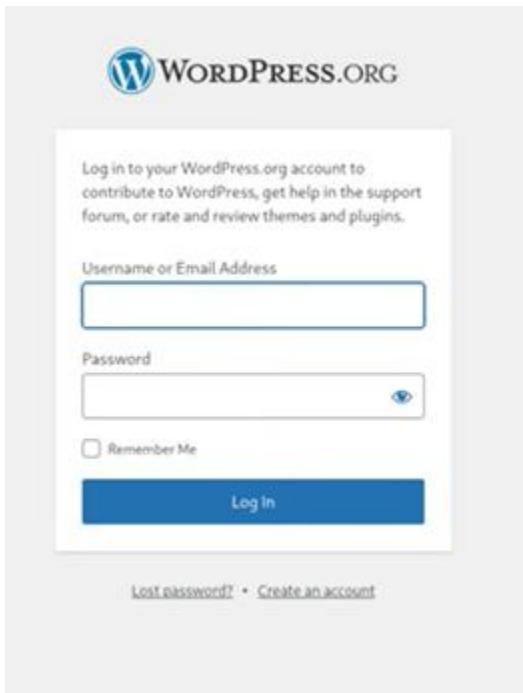
At the bottom, there are two buttons: '99 About' and '00 Exit', followed by the prompt '[-] Select an option : █'.

```
Session Actions Edit View Help
EPHISHER 2.3.5
[01] Localhost
[02] Cloudflared [Auto Detects]
[03] LocalXpose [NEW! Max 15Min]

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

The screenshot shows the LocalExpose web application. The left sidebar has sections for Tunnels, Domains, Endpoints, Access, Billing, and Settings. The main area is titled "Accessing local tunnel via CLI token". It lists three options: "Red Hat / CentOS / Fedora (Linux)" (selected), "Arch Linux (.pk3.tar.xz)" (disabled), and "Binary download for Linux" (disabled). Each option has a dropdown for "Select an arch" and a "Download" button. Below this is a "Access Token" section with a "Copy your access token" button and a redacted token field. At the bottom is a "Login" section with a "Log in using the access token above through the CLI or GUI" link.

```
Session 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... █
```



## 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.