Phishing Simulation Report

Cybersecurity Audit Project – Employee Vigilance Assessment

Organization

Confidential

Date

January 2026

Prepared By

Adebayo Fijabi

(Cybersecurity Analyst)

1 · Overview

A live phishing simulation was conducted to evaluate employee vigilance against credential-harvesting attacks following a phishing awareness training program. The exercise focused on reducing malicious link-click rates, minimizing credential submission attempts, and improving timely incident reporting through the organization's security channels.

2 · Objectives

- Reduce the rate of malicious link-clicks among targeted employees.
- Increase the number of phishing incident reports submitted to the security team.
- Minimize credential submission attempts on simulated phishing landing pages.

3 · Compliance Drivers

This initiative aligns with **ISO/IEC 27001** user awareness and training controls (Annex A 6.3), which require organizations to implement measurable security education programs. The phishing simulation supports this requirement by providing quantifiable metrics on employee susceptibility to social engineering attacks and tracking risk reduction progress through the organization's internal risk register.

4 · Tooling

- **Zphisher** – Used to generate the phishing simulation landing page and capture interaction metrics, including link clicks and credential submission attempts.
- **Localxpose** – optional port-forwarding for internal access during testing.
- **Google Sheets** – Used to track key performance indicators (KPIs) such as click-through rates, credential submissions, and incident reporting metrics.

5 · Simulation Scenario

A crafted invoice reminder email was delivered to targeted users, impersonating a WordPress service provider and requesting payment for website development services. The message contained a malicious payment link that redirected recipients to a cloned authentication page hosted via Zphisher, designed to simulate a real-world credential harvesting attack.

The scenario replicated common business email compromise (BEC) techniques used in financial phishing campaigns, including urgency, financial pressure, and trusted vendor impersonation.

5.1 · Phishing Email Template

Dear Alex,

I hope this message finds you well. This is a friendly reminder regarding the payment for the WordPress service provided on Enterprise Rebranding.

Invoice Details:

- **Service:** WordPress Design and Development
- **Amount Due:** $2572.59
- **Invoice Number:** CkGo502HID
- **Due Date:** 01/20/2025

Please click on this Link to arrange payment and see if you qualify for our yearly one time fee waiver by the due date to ensure uninterrupted service and continued support.

If the payment has already been processed, kindly disregard this message. Should you have any questions or require a copy of the invoice, feel free to reach out.

Thank you for your prompt attention to this matter.

Best regards,
WordPress Team.

6 · Metrics

Key Performance Indicator KPI	Baseline (Pre-Training)	Post-Campaign
Link click Rate	80 %	30 %
Credential submission Rate	60 %	20 %
Phishing Incident reporting	10 %	80 %

7 Analysis

- Link click rate decreased by **50 percentage points**, indicating a substantial improvement in user caution and recognition of suspicious emails.
- Credential submission attempts declined by **40 percentage points**, demonstrating stronger user skepticism toward deceptive login requests.
- Phishing incident reporting increased by **70 percentage points**, reflecting a shift toward proactive security behavior and improved security awareness culture.

7.1 Security Impact

The results confirm that the phishing awareness training and simulation significantly strengthened the organization's human security layer, reducing exposure to credential harvesting, business email compromise (BEC), and account takeover threats.

8 · Recommendations

- Conduct quarterly phishing simulations to sustain employee awareness and continuously reinforce secure behavior against evolving social-engineering tactics.
- Provide targeted refresher training for users who clicked malicious links or submitted credentials, ensuring focused remediation where risk exposure is highest.
- Publish real-time phishing metrics on the security operations dashboard to provide leadership with immediate visibility into organizational risk posture and user behavior trends.

8.1 Program Maturity Alignment

These recommendations support the development of a continuous security awareness program, aligning with industry best practices under ISO 27001, NIST CSF, and NIST 800-53 security control frameworks.

9 · Conclusion

The phishing simulation delivered measurable evidence of improved employee vigilance and strengthened human-layer defenses against credential harvesting and social engineering attacks. The results validate the effectiveness of the security awareness program and support continued investment in user focused security controls.

This initiative aligns with **ISO/IEC 27001** security awareness requirements and reinforces the organization's risk management objectives by reducing exposure to phishing, account compromise, and business email compromise (BEC) threats.