
Phishing Simulation Report

Cybersecurity Audit Project – Employee Vigilance Assessment

Organization: Confidential

Date: 02 July 2025

Prepared By: Awe O. Peter (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.

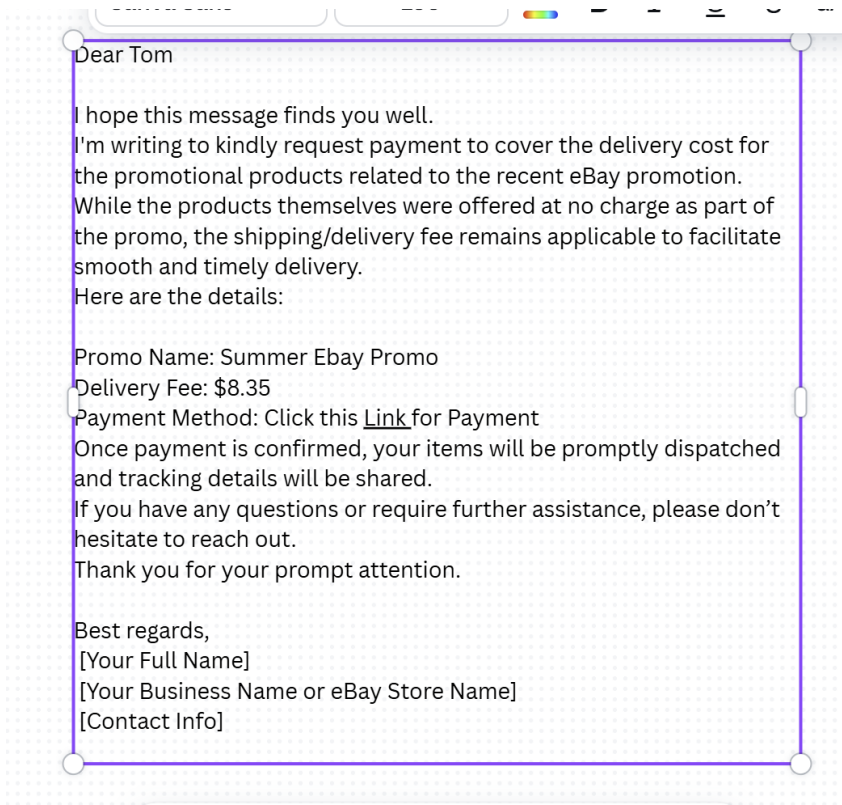
4 • Tooling

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

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.

5.1 • Phishing Email Template



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.

- 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.

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.