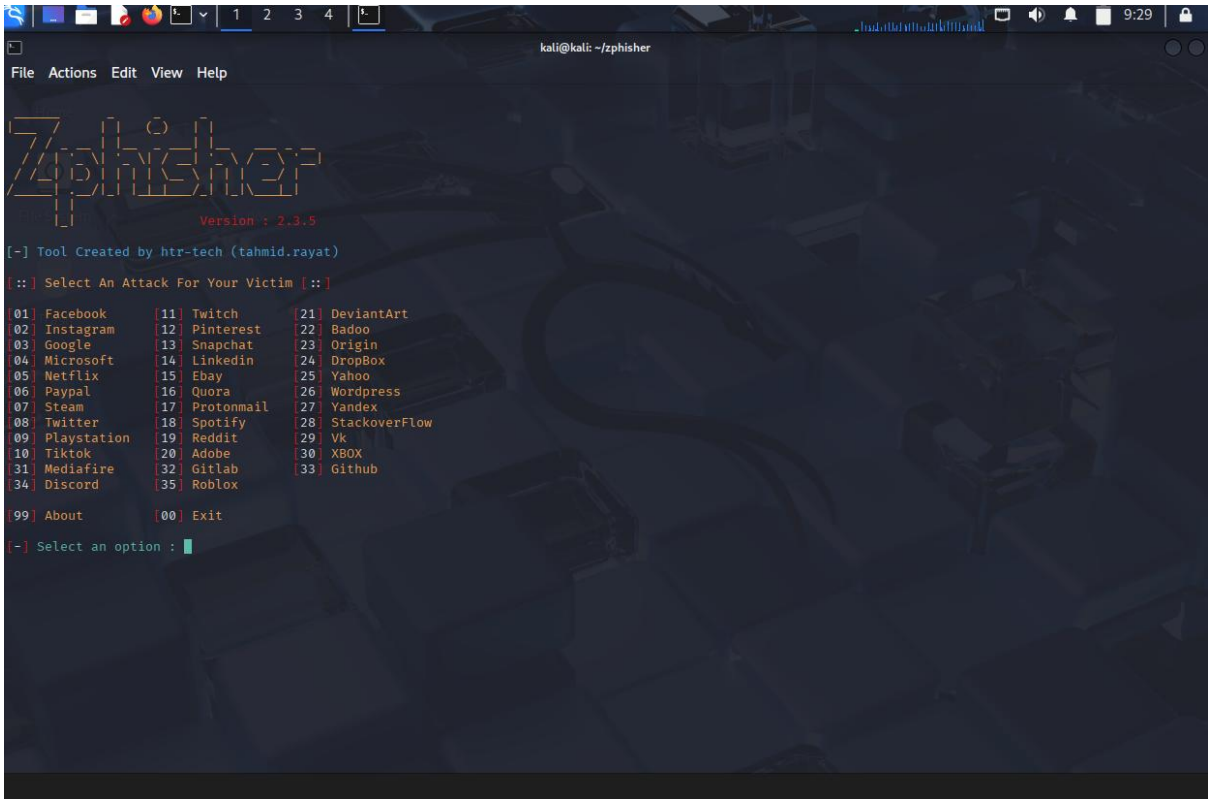
Phishing Simulation Report

Cybersecurity Awareness & Employee Vigilance Assessment

Organisation: Jaytech
Date: 23 Nov. 2025
Prepared By: Julius Ayobami Olasunkanmi

Phishing Simulation Interface Overview



The main interface utilized throughout the phishing simulation exercise is seen in the screenshot above.

The cybersecurity team was able to:

- Make controlled, realistic phishing pages
- Create many credential-harvesting scenarios.
- Keep a safe eye on employee relations
- Gather behavioural data for analysis.

The organization made sure that no actual data, infrastructure, or user credentials were ever exposed by utilizing a restricted simulation interface. The setting offered a consistent, secure, and safe way to gauge employee awareness.

OVERVIEW

To gauge staff awareness and behavioural reactions to possible credential-harvesting attempts, a live phishing simulation was carried out. The simulation was a component of the organization's larger cybersecurity awareness campaign, which aims to lower the danger of social engineering and increase alertness.

❖ THE MAIN FOCUS OF THE EXERCISE INCLUDED

Reducing the frequency of clicking on risky links

Cutting down on attempts to submit credentials

A rise in the quantity of phishing incidents that are reported to the security team

❖ OBJECTIVE

The following quantifiable results were the simulation's goals:

Reduce the percentage of participating employees that click on links

Boost the cybersecurity team's reporting of phishing incidents

Decrease the number of credentials submitted on phishing-like websites

These goals are in line with user security education best-practice improvement aims.

❖ COMPLIANCE DRIVER

Several governance and compliance criteria are directly supported by this phishing-simulation program:

ISO/IEC 27001 (Annex A 6.3) requires user awareness training to be organized and quantifiable.

The Internal Cyber Risk Register monitors the progress of risk mitigation related to social engineering.

Security Governance Frameworks: Make sure that human-factor vulnerabilities are continuously monitored and improved.

Demonstrating metrics from actual simulations improves regulatory compliance and audit readiness.

❖ TOOLING USED IN THE SIMULTION

The following resources were used to carry out a safe and efficient exercise:

- **Zphisher**

  used to create phishing websites and record non-sensitive interaction data, like clicks and submission attempts.
- **LocalXpose**

During internal testing, secure port forwarding was made available as an option to enable access to the simulated phishing pages.

- **Google Sheets**

  Key performance indicators (KPIs) from the simulation results are stored, monitored, and analyzed using this method.

These instruments guaranteed the simulation's continued safety, control, and complete isolation from real-world settings.

❖ SIMULATION SCENARIO

A phishing scenario was created wherein staff members were sent to a replicated sign-in page that looked like a genuine service.
Without revealing any actual systems, the goal was to mimic a credential-harvesting assault.

SCENARIO MEASURED

Link-clicking actions

Entered credentials (no stored data, just attempts)

Reporting employee actions

This configuration functioned as a practical assessment of staff alertness and compliance with security-training objectives.

KPI Category	Baseline (Before Awareness Training	Post-Simulation Result
Link Clicks	80%	20%
Credential Submissions	70%	10%
Phishing incident reports	10%	90%

Following the training program, these indicators show notable behavioral improvements.

❖ ANALYSIS REPORT

The findings point to a number of significant trends:

Decrease Unsafe Link Click:

Employees are now more cautious when connecting with unfamiliar or dubious connections, as seen by a significant decrease (60 percentage points).

Reduction in credential submission attempts:

A 60-point drop indicates a better capacity to spot phony login sites and prevent credentials from being compromised.

Significant in Reporting Behaviour:

A greater security culture and a desire to interact with the cybersecurity team are demonstrated by the rise from 10% to 80%.

All things considered, the simulation shows that the training program effectively increased staff awareness and decreased vulnerability to phishing threats.

RECOMMENDATIONS

The following steps are advised in order to preserve and enhance cybersecurity awareness:

1. Set Up Phishing Simulations Every Three Months:

Frequent practice helps spot new gaps and reinforces learnt behaviour.

2. Conduct Focused Refresher Training:

Additional training modules should be sent to anyone who clicked links or tried to submit their credentials.

3. Expand Simulations type:

Add versions like:

Smishing SMS

Phishing (quishing) using QR codes

Voice-based vishing

4. Phishing scenario on social media:

Include KPI dashboards

Show leadership and security teams real-time phishing simulation metrics.

5. Ongoing Micro-Training:

Maintaining long-term awareness is facilitated by brief, regular learning modules.

❖ CONCLUSION

Clear, measurable proof of increased employee cybersecurity knowledge was shown by the phishing simulation.
Workers showed enhanced reporting behaviour, greater skepticism of dubious content, and improved judgment.