

Phishing Simulation Report

Cybersecurity Audit Project – Employee Vigilance Assessment

Prepared by: Dada Ojuko
(Cybersecurity Analyst)

Date: December 2025

1. Overview

Phishing simulations are controlled, ethical cybersecurity exercises designed to evaluate how well employees can recognize and avoid deceptive messages that attempt to steal sensitive information. These simulations helped our organizations identify awareness gaps, reinforce best practices, and strengthen their overall security posture.

Tools such as **Zphisher** and **LocalXpose** was used **in a safe, internal, and legal testing environment** to replicate real-world attack patterns without exposing the organization to actual threats.

2. Purpose of the Simulation

The objective is to:

- Measure employee susceptibility to phishing attempts.
- Assess how users respond to unexpected login prompts, suspicious links, or credential requests.
- Reduce credential submission attempts on the phishing landing page.
- Identify departments or roles with higher risk.
- Strengthen security culture through feedback and training.

This assessment ultimately helps reduce the risk of data breaches caused by social engineering.

3. Compliance Drivers

The phishing simulation was in compliance with **ISO/IEC 27001 Annex A 6.3** which requires organizations to ensure that all users understand their information-security responsibilities and are equipped to recognize, prevent, and report security threats. This control focuses on maintaining a continuous program of security awareness that covers policies, acceptable use, data protection requirements, and emerging risks such as phishing or social-engineering attacks.

Our organization provided regular training, deliver targeted awareness materials, and reinforce secure behaviours through reminders, assessments, and role-specific education. The goal is to ensure that every user—employees, contractors, and relevant third parties—contributes to the protection of information assets and reduces the likelihood of human-related security incidents.

4. Tools used in the Simulation

a) Zphisher (for Crafting Phishing Pages)

Zphisher is an open-source toolkit that automates the creation of phishing landing pages mimicking common services (e.g., email portals, cloud services). In simulations, it can be used to:

- Generate a realistic mock phishing login page.
- Track when employees click links or attempt to enter credentials (without storing real passwords).
- Customize templates to match the organization's internal ecosystem.

b) LocalXpose (for Secure Tunneling and Hosting)

LocalXpose is a reverse-proxy tunneling tool that allows internal servers or mock webpages to be temporarily exposed for testing.

During a simulation, it can:

- Host the phishing simulation page without deploying a public server.
- Obscure internal URLs with safe, temporary public links.
- Provide HTTPS tunnels for more realistic scenarios.
- Offer monitoring logs to track user interactions.

c) Google Sheets – Used to stored KPIs.

5. Phishing Simulation Scenario – Facebook & Yahoo Login Themes (Using Zphisher).

In this phishing-awareness simulation Zphisher was used to generate realistic, **mock** Facebook and Yahoo login pages for training purposes. The scenario is designed to assess how employees respond to deceptive prompts that mimic common social-media and email login screens—two frequent targets in real-world attacks.

Participants receive a controlled, permission-based test email containing a link to the simulated page. When users click the link or attempt to enter credentials, the system records interaction metrics **without storing real passwords**. The results help identifies awareness gaps, reinforce safe practices such as checking URLs and reporting suspicious messages, and strengthen the organization's overall defence against social-engineering attacks.

❖ “Security Notice: Confirm Recent Login Activity” (Facebook-themed Simulation):

Subject: Action Required: Review Recent Login Activity on Your Account

Hello Susan,

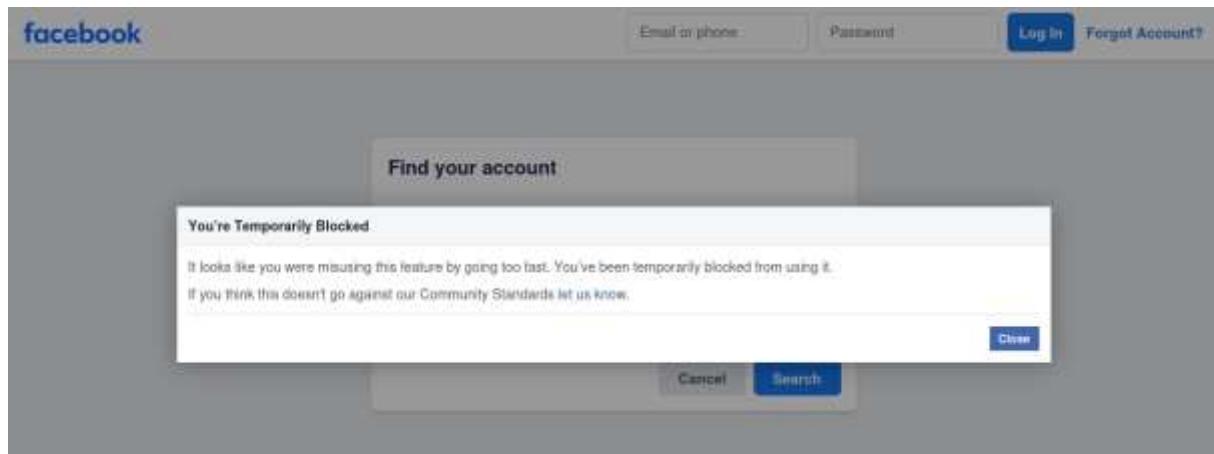
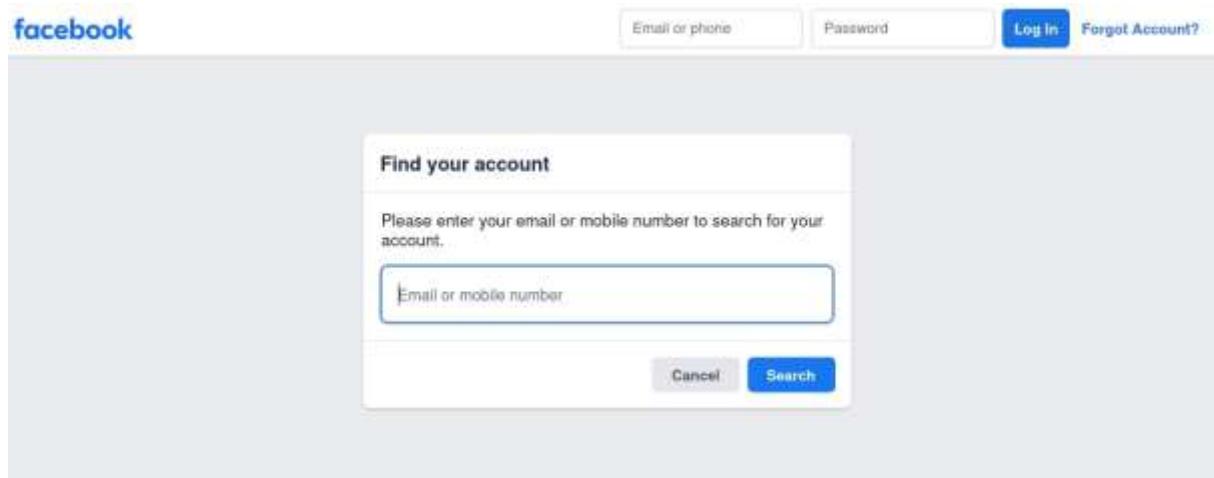
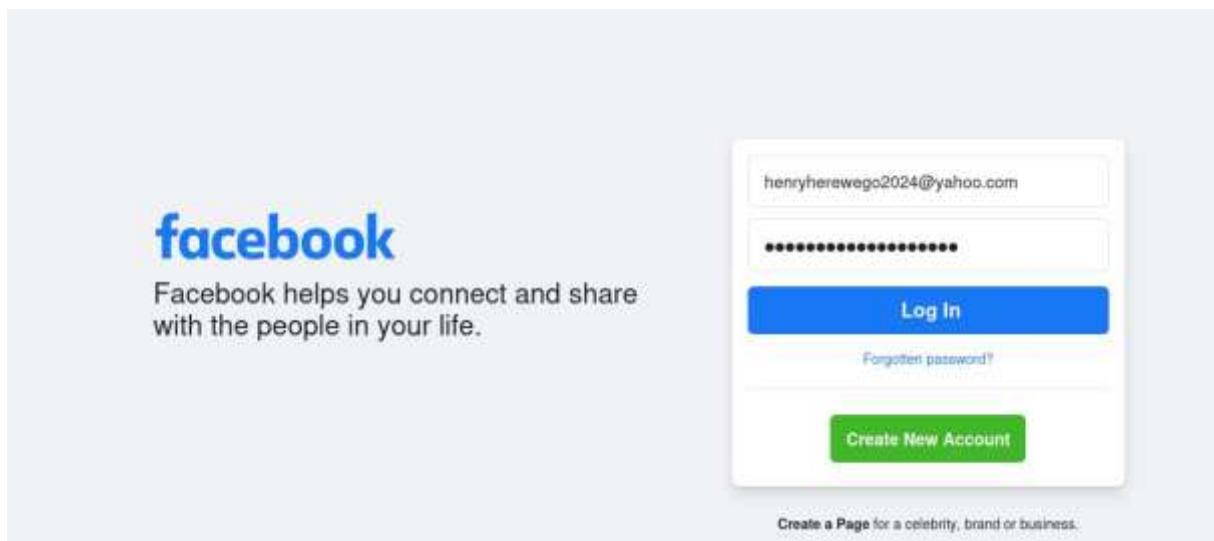
We detected a new login attempt to your Facebook account from an unrecognized device. For your security, please review the activity and confirm whether it was you.

Review Activity:

Click [Verify Login Activity](#) to continue to the verify process.

If this was not you, we recommend confirming your account settings as soon as possible.

*Thank you,
Facebook Security Team*



```
[+] Login info Found !!
[+] Account : henryherewego2024@yahoo.com
[+] Password : Itsjus$tmehere2025$
```

❖ “Mailbox Storage Alert” (Yahoo-themed Simulation):

Subject: Your Yahoo Mailbox Is Almost Full

Dear Adrian,

Your Yahoo mailbox has reached **95% capacity**. Incoming messages may be delayed unless you free up space or revalidate your mailbox settings.

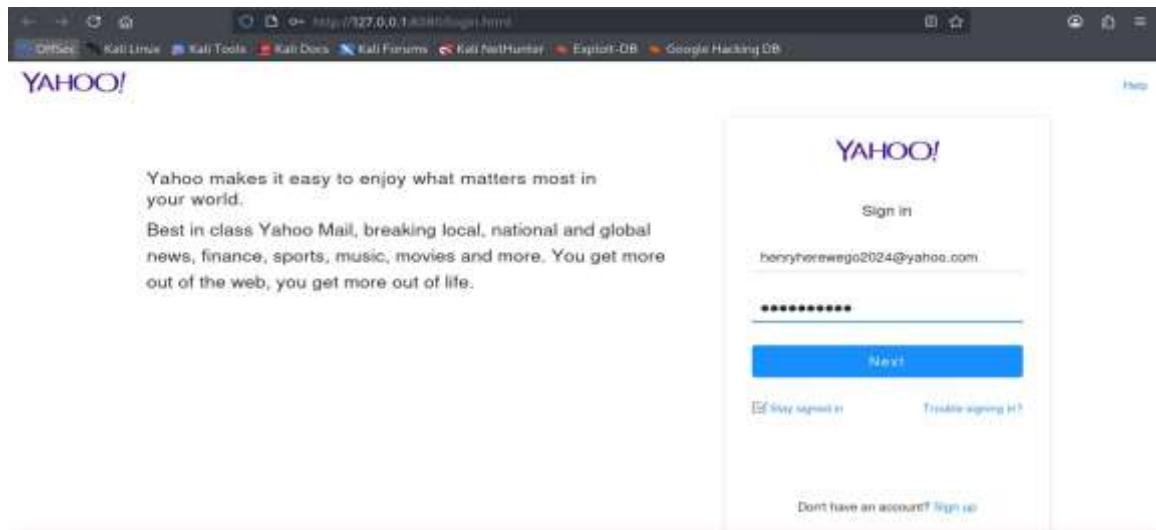
To continue receiving emails without interruption, please confirm your mailbox status:

Check Mailbox Status:

Please click [Update Mailbox](#) to continue the process.

Thank you for keeping your account up to date.

Regards,
Yahoo Mail Services





```
[+] Login info Found !!
[+] Account : henryherewego2024@yahoo.com
[+] Password : Comment23$
```

6. Metrics

The phishing simulation was evaluated using three primary KPI metrics: **link clicks**, **credential submissions**, and **phishing reports**.

- ❖ **Link Clicks:** measure how many users interacted with the simulated phishing message, indicating initial susceptibility to deceptive links.
- ❖ **Credential Submissions:** represent instances where users attempted to enter login details on the mock phishing page, highlighting higher-risk behaviour and gaps in verification practices.
- ❖ **Phishing reports:** track how many users correctly identified the message as suspicious and reported it through approved channels.

Together, these KPI metrics provided a clear view of user awareness levels, enabling the organization to identify training needs, measure progress over time, and strengthen overall security posture.

KPI	Baseline	Post-Campaign
Link clicks	85 %	35 %
Credential submissions	80 %	15 %
Phishing reports	10 %	85 %

7. Simulation Analysis

- ❖ **Link-click frequency decreased by fifty percentage points**, indicating improved user caution.
- ❖ **Credential submission attempts declined by sixty-five percentage points**, showing heightened scepticism toward suspicious prompts.
- ❖ **Reporting rate increased by seventy-five percentage points**, demonstrating more proactive security behaviour.

8. Benefit of This Approach

- ❖ Real-world readiness by exposing employees to believable attack scenarios.
- ❖ Data-driven security improvements through measurable results.
- ❖ Strengthened organizational culture regarding cyber hygiene.
- ❖ Reduced breach risk by training humans, who are often the weakest link.

9. Recommendations

- ❖ **Reinforce Targeted Awareness Training**

Continue delivering focused training sessions for teams or individuals who demonstrated higher click rates or lower reporting activity. Tailor content toward recognizing suspicious URLs, hovering over links, and validating sender authenticity.

❖ **Increase Frequency of Micro-Simulations**

Deploy shorter, periodic phishing simulations to maintain vigilance and ensure improvements remain consistent over time. Vary themes and difficulty levels to reflect evolving real-world threats.

❖ **Strengthen Reporting Culture**

Encourage employees to treat reporting as a first-line defense. Promote easy-to-use reporting channels, integrate one-click reporting tools, and recognize employees who consistently demonstrate good security habits.

❖ **Enhance Role-Based Security Guidance**

Provide specialized training for high-risk roles such as finance, HR, and administrative personnel, who often receive more targeted phishing attempts.

❖ **Embed Security Messaging Into Daily Workflows**

Use internal newsletters, visual reminders, and periodic alerts to reinforce key phishing-awareness principles and maintain a culture of continuous security consciousness.

10. Conclusion

The phishing simulation results showed meaningful progress in employee security vigilance awareness, with notable reductions in link-click activity and credential submission attempts alongside a significant rise in reporting behaviour. These trends indicate growing scepticism toward suspicious messages and a stronger organizational commitment to proactive security practices.

By continuing to invest in awareness training, frequent simulations, and a supportive reporting environment, the organization can further reduce human-factor risks and enhance its overall cybersecurity resilience.