Phishing Simulation Report

Cybersecurity Audit Project
Employee Vigilance Assessment
Organisation: Confidential

Prepared By:
Junaid AbdulRahman A
Cybersecurity Analyst

Date:27 November 2025

1 · Project Overview

A live phishing simulation was conducted to measure 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

To access the susceptibility of employees to phishing attack and evaluate the effectiveness of the phishing awareness training and also identify ares for improvement to enhance the overall security posture

3 · Compliance Drivers

ISO 27001 Annex A 6.3: Information security awareness, education and training demands measurable security education, while the internal risk register tracks progress against social-engineering risks.

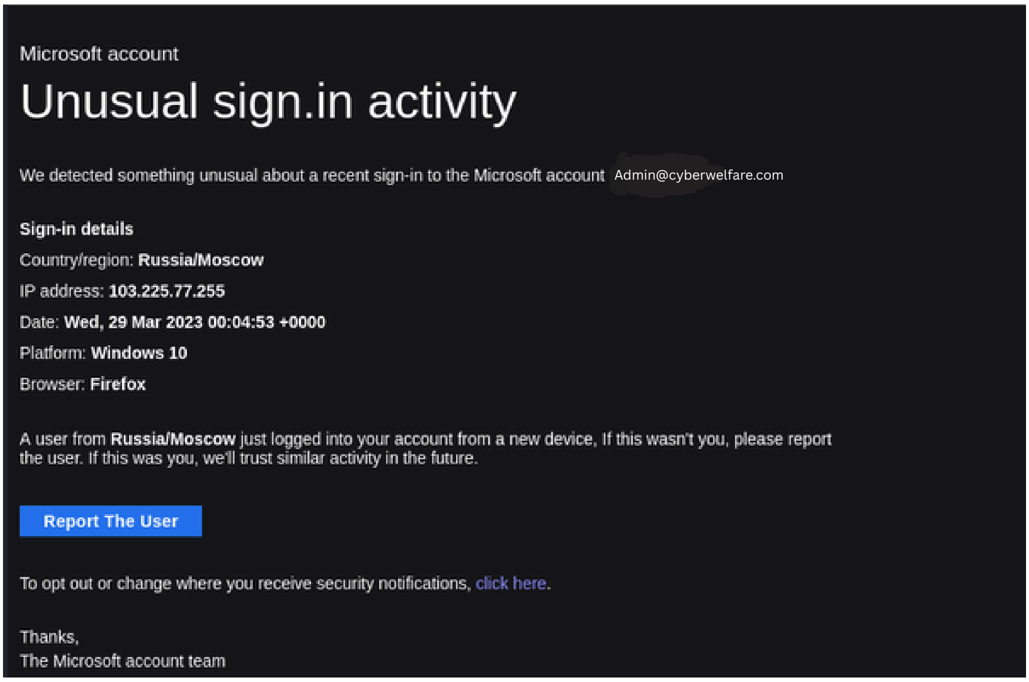
4 · Tools Used

- Zphisher – Used to generate the phishing site and capture interaction data.
- Localxpose – optional port-forwarding for internal and external access during testing.
- Google Sheets – stored key performance indicators.

5 · Simulation Scenario

A crafted unusual sign in activity email was sent requesting recognition of the activity of signing into the Microsoft account. The message included a link that directed recipients to a clone login page hosted with Zphisher.

5.1 · Phishing Email Template



Microsoft account

Unusual sign.in activity

We detected something unusual about a recent sign-in to the Microsoft account Admin@cyberwelfare.com

Sign-in details

Country/region: **Russia/Moscow**

IP address: **103.225.77.255**

Date: **Wed, 29 Mar 2023 00:04:53 +0000**

Platform: **Windows 10**

Browser: **Firefox**

A user from **Russia/Moscow** just logged into your account from a new device, If this wasn't you, please report the user. If this was you, we'll trust similar activity in the future.

Report The User

To opt out or change where you receive security notifications, click here.

Thanks,
The Microsoft account team

6 · Metrics

KPI	Pre-Campaign	Post-Campaign
Link Clicks	80%	20%
Credential Submissions	70%	15%
Phishing Report	10%	80%

7 · Analysis

- Link-click frequency fell by sixty percentage , reflecting greater caution.
- Credential submission attempts dropped by fifty-five percentage, indicating stronger vigilance.
- Reporting rate rose by seventy percentage, demonstrating proactive security behavior.

8 · Recommendations

- Schedule quarterly phishing simulations to maintain awareness.
- Provide additional training for employees who continue to click on phishing links.
- Display live report metrics on the security dashboard for immediate visibility.

- Implement technical controls such as email filters and anti-phishing software, to reduce numbers of phishing emails reaching employees inboxes.
- Review and update the organization email usage policy to include phishing prevention guidelines.

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.

The simulation has also provide valuable insight into the organization vulnerability and strength. By creating cybersecurity awareness culture would help the organization reduce risk of phishing attack.