# Phishing Simulation Report

## Cybersecurity Audit Project – Employee Vigilance Assessment

**Organization: Confidential**

**Prepared By: Dayo Sonibare (Cybersecurity Analyst)**

**Date: 2nd July, 2025.**

## Overview

A live phishing simulation measured employee vigilance against credential-harvesting attacks after a phishing-awareness training program. The exercise focused on lowering link-click frequency, reducing credential submission attempts, and improving incident reporting.

## 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.

## 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.

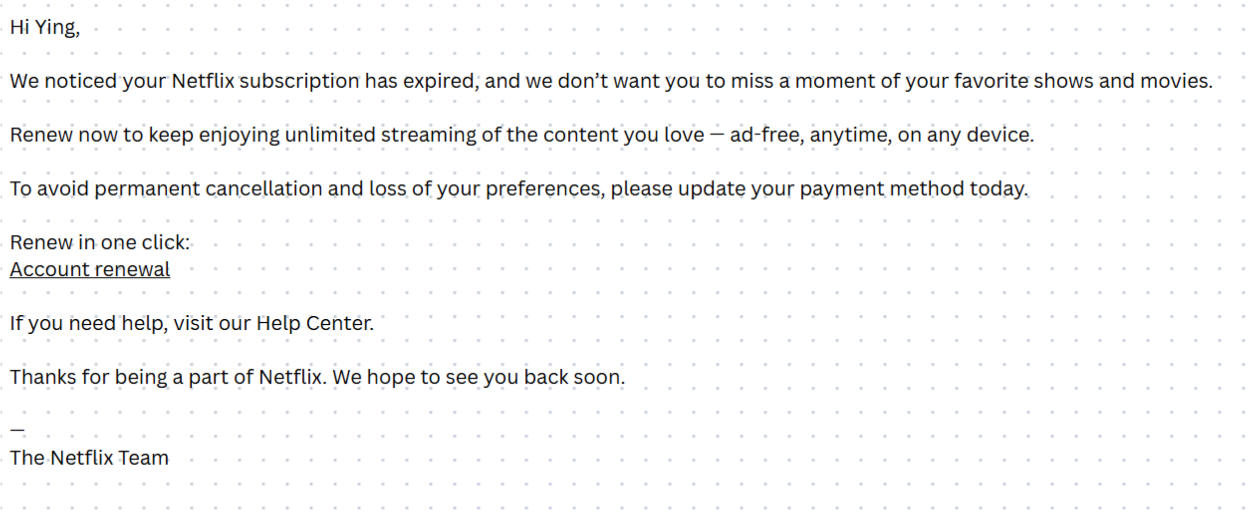
## Tooling

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

## Simulation Scenario

A crafted reminder email requested payment for Netflix subscription. The message included a link that directed recipients to a clone login page hosted with Zphisher.

## Phishing Email Template



Hi Ying,

We noticed your Netflix subscription has expired, and we don’t want you to miss a moment of your favorite shows and movies.

Renew now to keep enjoying unlimited streaming of the content you love — ad-free, anytime, on any device.

To avoid permanent cancellation and loss of your preferences, please update your payment method today.

Renew in one click:
Account renewal

If you need help, visit our Help Center.

Thanks for being a part of Netflix. We hope to see you back soon.

—
The Netflix Team

### Metrics

| KPI | Baseline | Post-Campaign |
|---|---|---|
| Link clicks | 80 % | 30 % |
| Credential submissions | 60 % | 20 % |
| Phishing reports | 10 % | 80 % |

### Analysis

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

### 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.

### 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.