

Project Report: Phishing Simulation Campaign

Conducted by: NymousTechnologies

Date: 20-10-2025

Project Lead: Samsudeen Olapade

1. Introduction

As part of NymousTechnologies' ongoing efforts to strengthen organizational cybersecurity awareness and resilience, a **Phishing Simulation Campaign** was launched targeting employees in the **Sales, Marketing, and IT departments**. The objective of this campaign was to evaluate the effectiveness of the prior phishing awareness training and to measure improvements in employee vigilance, response behavior, and reporting practices.

2. Objectives

The key objectives of the campaign were:

- To assess employees' ability to identify and respond appropriately to phishing emails.
- To evaluate the effectiveness of the previous phishing awareness training.
- To measure changes in phishing susceptibility across key departments.
- To identify areas requiring further security awareness reinforcement.

3. Target Audience

The phishing simulation targeted a total of **105 employees** across three departments:

- **Sales Department:** 35 employees
- **Marketing Department:** 30 employees
- **IT Department:** 40 employees

These departments were selected due to their frequent engagement with external communications, making them prime targets for real-world phishing attempts.

4. Simulation Design and Execution

The simulation was designed to mimic a **credential-harvesting phishing attack**, one of the most common and impactful phishing vectors.

- **Phishing Vector:** Email with a link to a **cloned login portal**.
- **Email Theme:** A realistic message designed to prompt users to log in urgently e.g. account verification.

Update Your PayPal Login Details

Hi John,

We hope you're doing well. This is a quick reminder that your PayPal account login details may need updating to ensure continued access and account security.

To proceed, please log in to your PayPal account directly [here](#) and follow the prompts to update your username and password if necessary.

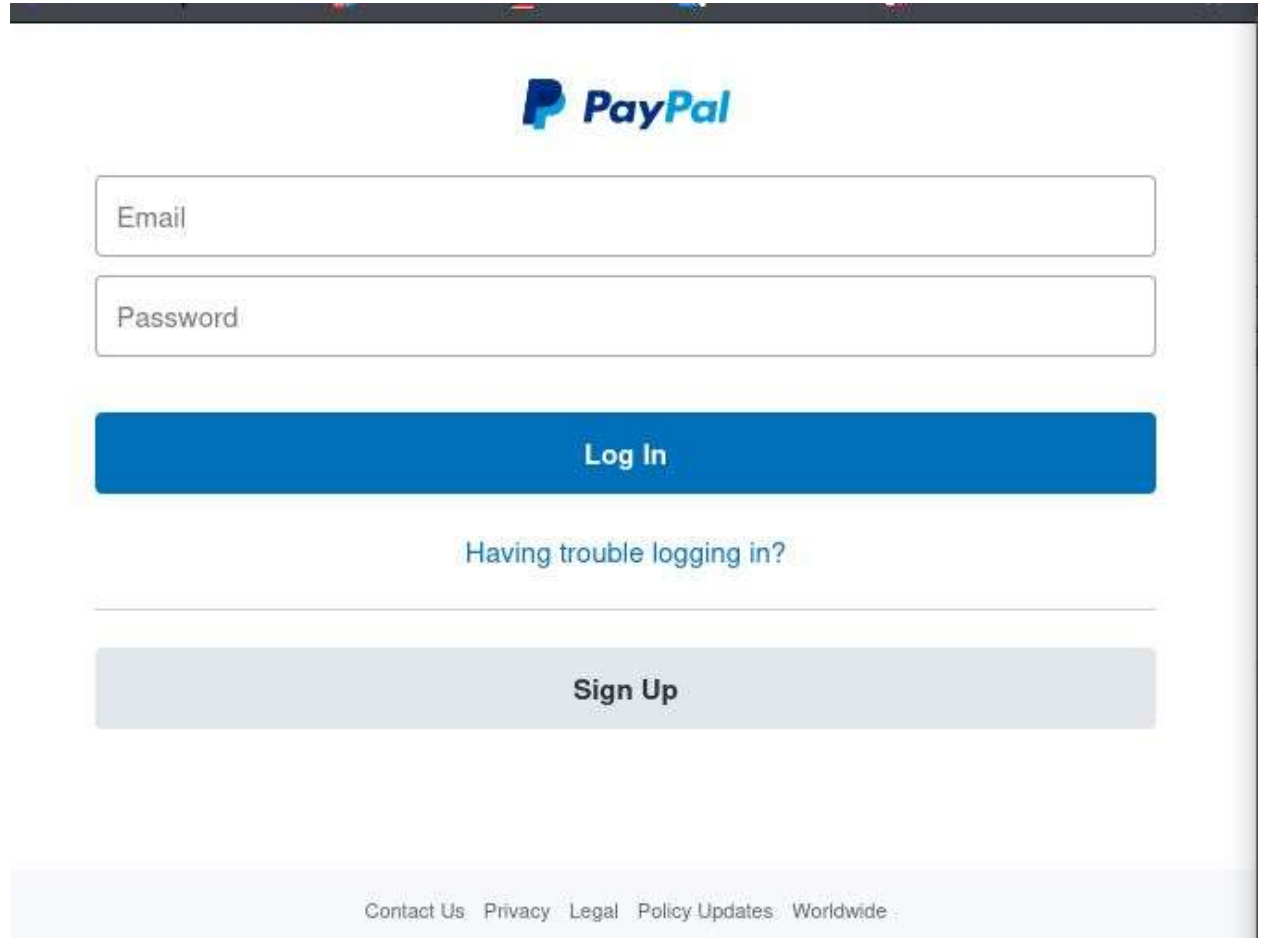
For your safety, please do not click on any links from unknown sources or share your login credentials via email.

Let us know once you've completed the update or if you run into any issues.

Best regards,
The PayPal Team.



The login page below is what displays when the link in the image above is clicked.

A screenshot of the PayPal login page. At the top center is the PayPal logo. Below it are two input fields: the first is labeled 'Email' and the second is labeled 'Password'. Under the password field is a blue button with the text 'Log In'. Below the 'Log In' button is a link that says 'Having trouble logging in?'. Further down is a light blue button with the text 'Sign Up'. At the bottom of the page, there is a footer with links: 'Contact Us', 'Privacy', 'Legal', 'Policy Updates', and 'Worldwide'.

- **Data Points Collected:**
 - Email click rates
 - Credential submission rates
 - Incident reporting rates

The simulation was executed over a controlled period, ensuring accurate measurement of user actions and responses.

5. Results and Analysis

5.1 Pre-Training Results

Before the phishing awareness training was implemented, earlier simulations revealed concerning trends:

- **Click Rate:** ~35%
- **Credential Submissions:** 13%
- **Reporting Rate:** 10–12%

These figures indicated a significant susceptibility to phishing threats and a lack of proactive reporting behavior.

5.2 Post-Training Results

After delivering structured phishing awareness training sessions—covering topics such as recognizing phishing red flags, verifying URLs, and proper incident reporting—a follow-up simulation was conducted. The results demonstrated a notable positive shift:

- **Click Rate:** Reduced to **15–20%**
- **Credential Submissions:** Dropped to **almost 0%**
- **Reporting Rate:** Increased to **33–47%**

These outcomes highlight a substantial improvement in user awareness, vigilance, and incident reporting culture across the targeted departments.

6. Key Insights

- **Improved Awareness:** The sharp decline in click and credential submission rates indicates that employees are now more cautious when engaging with unsolicited emails.
- **Enhanced Reporting Culture:** The rise in reporting demonstrates growing confidence among staff in identifying and escalating potential threats.
- **Training Effectiveness:** The post-training performance validates the success of the awareness sessions and reinforces the importance of continuous education.

7. Recommendations

To sustain and further improve phishing resilience, the following actions are recommended:

1. **Regular Phishing Simulations:** Conduct quarterly simulations to maintain awareness and track progress.
2. **Targeted Refresher Training:** Provide additional support to departments or individuals exhibiting residual risk behavior.
3. **Gamified Awareness Programs:** Introduce reward-based incentives to encourage proactive reporting.
4. **Enhanced Technical Controls:** Continue implementing email filtering, multi-factor authentication, and URL inspection technologies to reduce exposure.

8. Conclusion

The phishing simulation campaign conducted by NymousTechnologies successfully demonstrated the positive impact of cybersecurity awareness training. Employees showed significant improvement in identifying, avoiding, and reporting phishing attempts. Continued engagement,

regular simulations, and reinforcement training will be essential to maintaining and enhancing the organization's human-layer defense against evolving phishing threats.

Prepared by:

Samsudeen Olapade

Role: Cybersecurity Analyst

Organization: NymousTechnologies