SIMULATED PHISHING ATTACKS USING GOPHISH: TESTING EMPLOYEES AWARENESS AND ENHANCING SECURITY TRAINING PROGRAMS.

AUTHOR

MAC-DONALD ONYEWUCHI EGBUNA

OBJECTIVES

The objective is to assess employee awareness by measuring their ability to recognize and respond appropriately to phishing attempts.

MAY 15, 2025

TABLE OF CONTENT

EXECUTIVE SUMMARY

This report outlines the implementation of simulated phishing attacks using Gophish, an open-source phishing framework, to test employee awareness and strengthen organizational security training programs. The objective is to assess employees' susceptibility to phishing attacks, identify vulnerabilities, and improve security awareness through targeted training. The report covers the setup process, campaign design, execution, results analysis, and recommendations for enhancing employee training based on outcomes. Gophish was selected for its flexibility, ease of use, and ability to simulate realistic phishing scenarios.[](https://getgophish.com/)

INTRODUCTION

Phishing remains a leading cyberthreat, exploiting human vulnerabilities to gain unauthorized access to sensitive data. Simulated phishing campaigns are a proactive approach to evaluate employee awareness and reinforce security best practices. Gophish, an open-source phishing toolkit, enables organizations to create, execute, and analyze phishing simulations in a controlled environment. This report details the methodology and findings of a Gophish-based phishing simulation conducted to enhance employee security training.

METHODOLOGY

Gophish Setup

Gophish was installed on a secure server to ensure controlled and safe execution of phishing simulations. The setup process included:

- **Installation**

  Downloaded Gophish from the official repository (getgophish.com). (https://getgophish.com/)

- **Server Configuration**

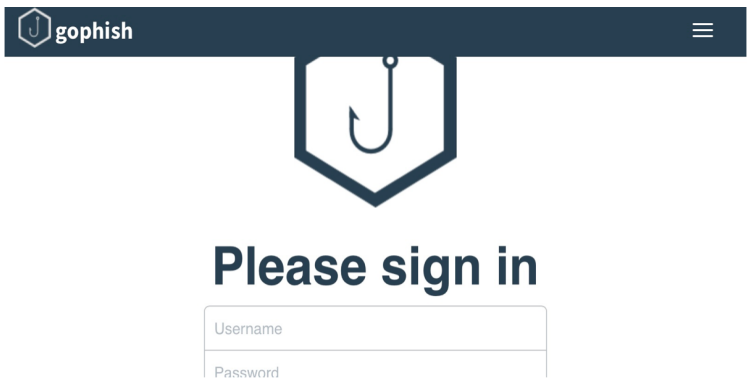
  - Set up a domain for sending phishing emails, ensuring proper DNS records (e.g., SPF, DKIM) to avoid spam filters.

  - Configured SMTP settings to integrate with a legitimate email service for realistic email delivery.

- **Security Measures**

  - Ensured all simulations were conducted in a controlled environment to avoid unintended data exposure.

  - Obtained management approval and informed IT teams to prevent flagging of simulated emails as real threats.



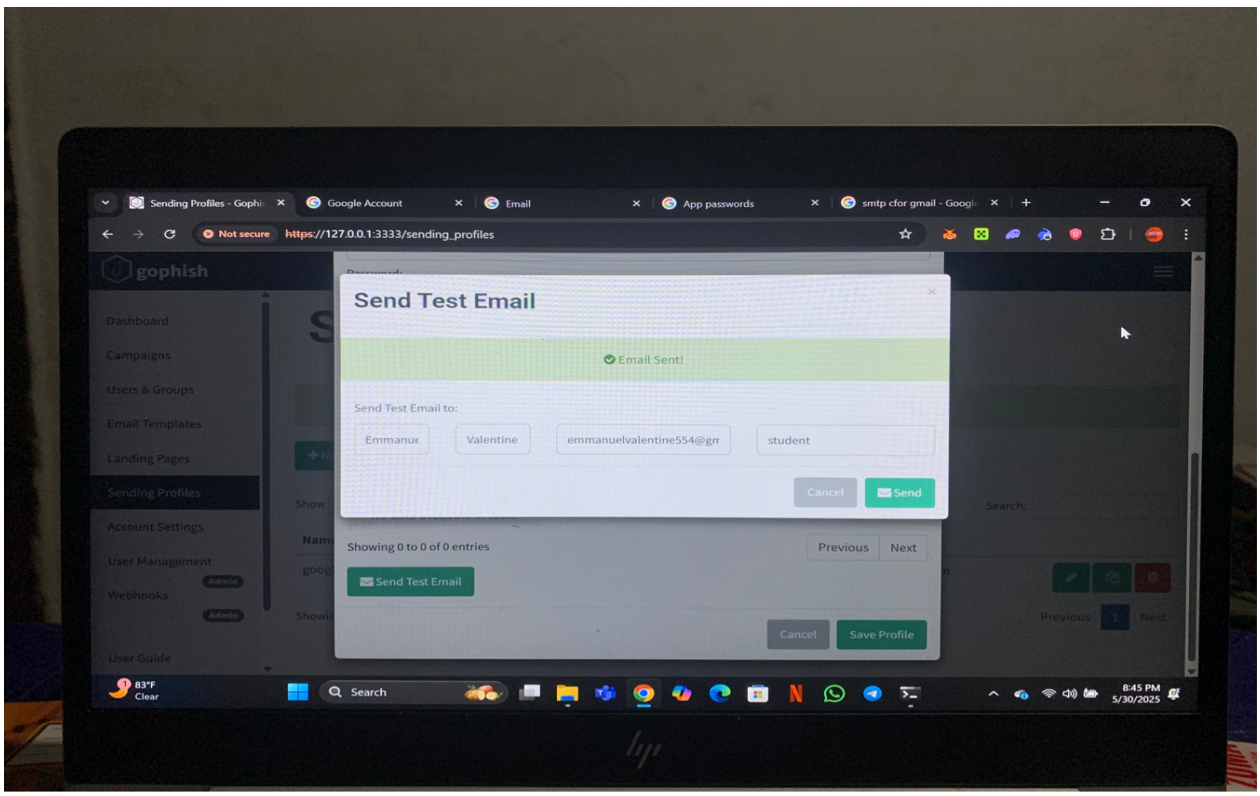
- **Campaign Design**

Three phishing scenarios were designed to test different aspects of employee awareness:

Sending Profile

In this aspect, the name used is Google Mail
SMPT : smpt.google.com;465
SMPT FROM; pppp000x0@gmail.com
Port used; 465 or 587 or 25
username: pppp000x0@gmail.com
Password: was gotten from the email "app password"

Then an email was sent to emmanuelvalentine554@gmail.com to verify the credibility of the gophish send profile

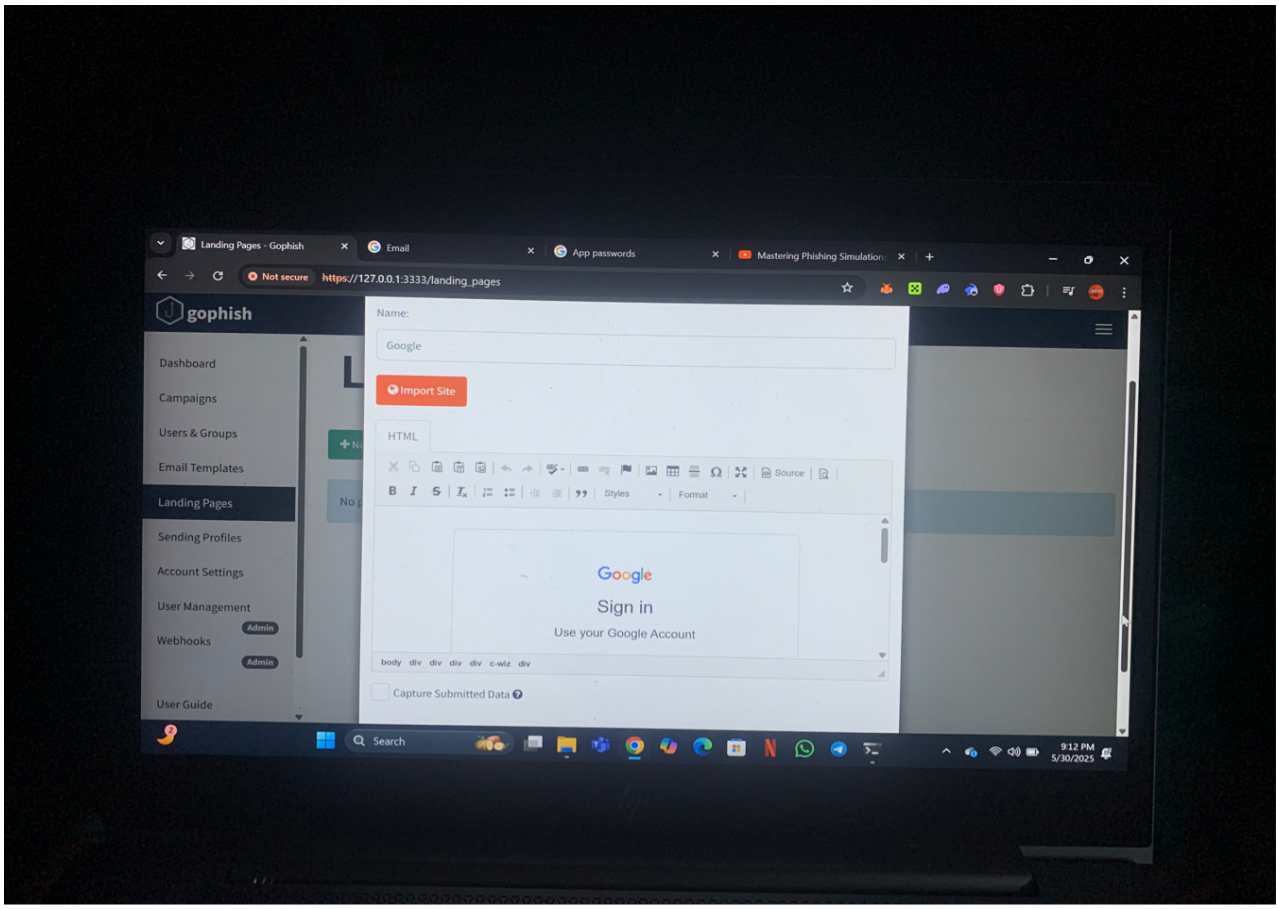


Land Profile

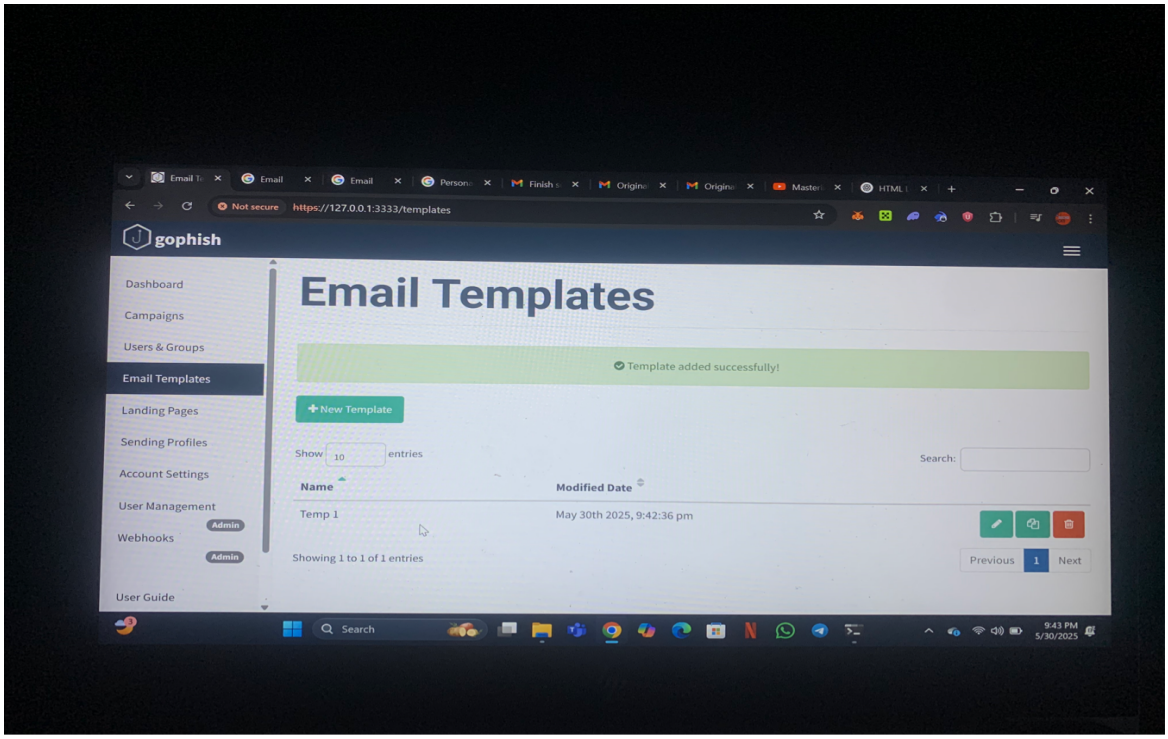
The following details below was required

Name : Google

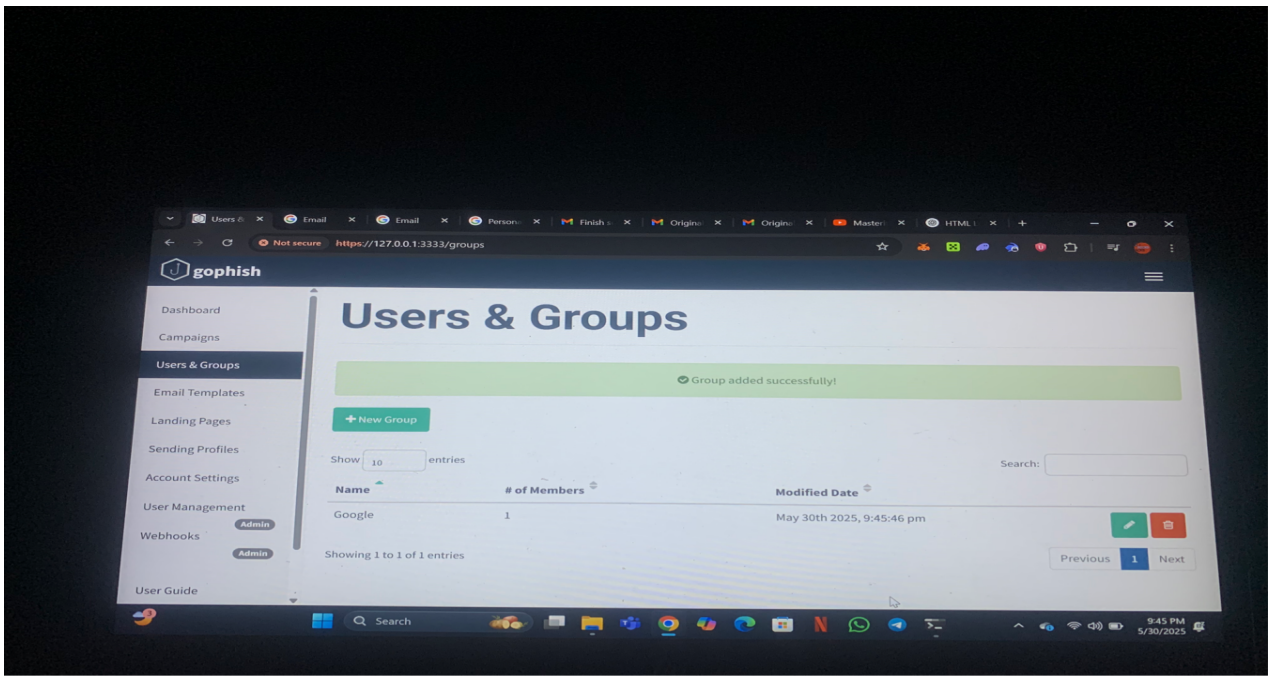
And the website https://myaccounts.google.com was imported



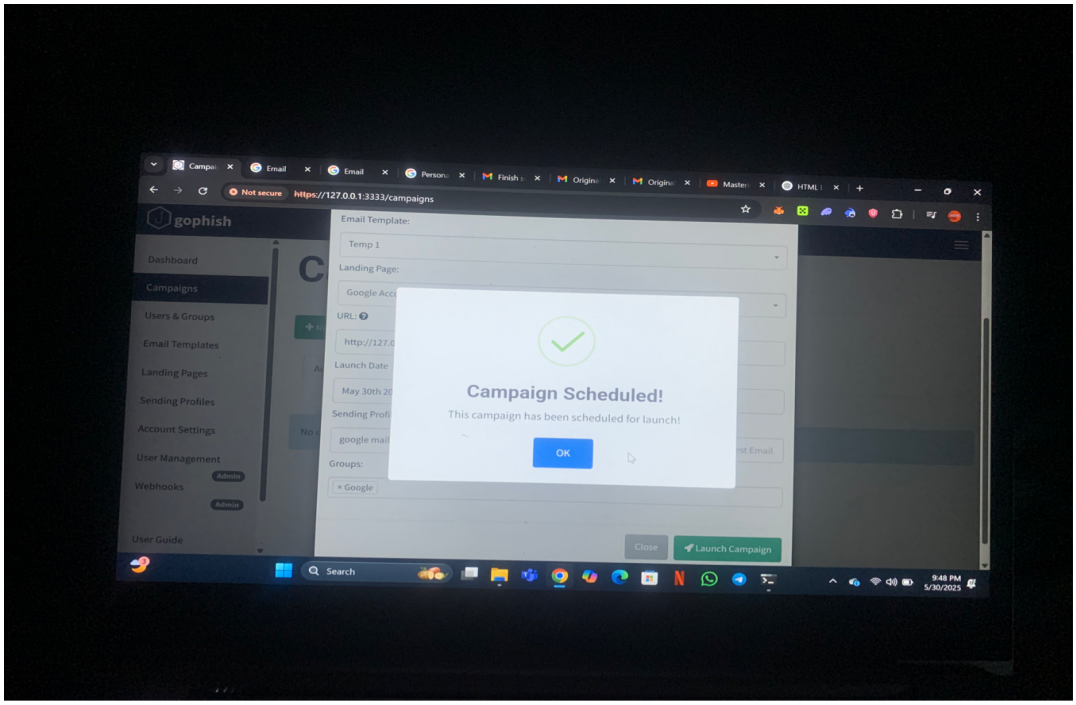
E-mail Template



Users and Groups



Campaign



- **Scenario**

A fake google mail login page prompted users to enter credentials due to a supposed account verification.

- **Objective** Test susceptibility to credential theft.

- **Email Template**: Mimicked Microsoft ' s branding with a sense of urgency (e.g., " Your account will be locked in 24 hours").

-**Landing Page**: A cloned google account login page hosted on the Gophish server.

- **Malicious Link**

- **Scenario**: An email posing as an urgent announcement enclosed by hyperlink "here"

- **Objective**: Measure click-through rates on suspicious links.

- **Email Template**: Used company branding with a generic subject line (e.g., Urgent need to authenticate your account failure to do so will lead to your account being terminated ").

- **Landing Page:** A google account page.

- **Campaign Execution**

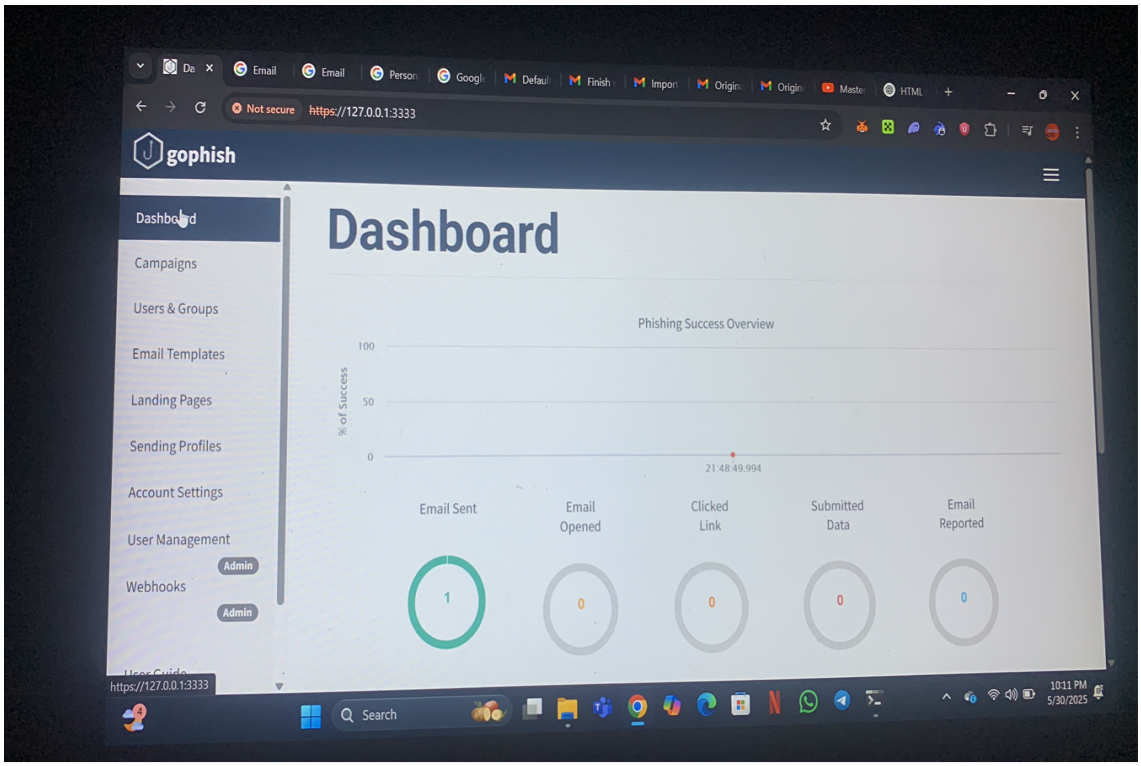
- Target Group: 2 employees across departments (IT, HR, Finance, Sales).

- Timeline: Campaigns ran for a week, with each scenario sent to a randomized subset of employees.

- Tracking: Gophish tracked email opens, link clicks, credential submissions

- Frequency: One email per employee per week to avoid pattern recognition.

- Ethical Considerations: Employees were informed post-campaign about the simulation to maintain trust.



Key Findings

-Awareness Gaps 5% of employees submitted credentials, indicating a critical need for training on recognizing phishing login pages.

- High Engagement: less than 10% email open rates suggest phishing emails were convincingly crafted, mimicking real-world threats.

-Departmental Variations: Finance employees were most susceptible, while IT showed strong awareness.

- Positive Behaviors:90% of employees reported suspicious emails, reflecting some level of vigilance.

- **Recommendations for Security Training**

Based on the simulation results, the following training enhancements are proposed:

Targeted Training for High-Risk Departments

- Develop Finance-specific modules focusing on credential harvesting and fake login page detection.
- Use real-world examples from the simulation to illustrate risks.

- **Benefits of Using Gophish**

- **Cost-Effective**: As an open-source tool, Gophish is free, making it accessible for organizations of all sizes. (https://getgophish.com/)

-Customizable Offers flexible email templates and landing pages to simulate diverse phishing scenarios.

- **Comprehensive Reporting**: Provides detailed metrics on email opens, clicks, and submissions for actionable insights.
- **Ease of Use**: User-friendly interface simplifies

Challenges and Mitigation

- **Challenge**: Employee backlash due to feeling "tricked" by simulations.

Mitigation: Communicate the purpose of simulations post-campaign and emphasize their role in improving
security.[](https://www.reddit.com/r/cybersecurity/comments/15yc6tx/phishing_simulation_backlash/)

Challenge False positives from automated systems skewing results.

Mitigation: Use Gophish ' s filtering tools to exclude automated interactions.[(https://keepnetlabs.com/blog/how-to-manage-false-clicks-in-phishing-simulations-for-security-awareness-training)

- **Challenge**: Crafting realistic emails without violating intellectual property (e.g., mimicking branded templates).

Mitigation: Use generic templates or seek legal guidance for branded simulations.

- **Conclusion**

The Gophish-based phishing simulation successfully identified employee awareness gaps and provided actionable data to enhance security training programs. The high engagement rates and varying departmental performance underscore the need for tailored training initiatives. By integrating regular simulations, interactive workshops, and policy updates, the organization can significantly reduce its phishing vulnerability. Gophish proved to be an effective, cost-efficient tool for simulating realistic phishing attacks and driving security awareness.