Phishing Awareness Executive Summary

Project: Phishing Attack Simulation (Gophish)
Author: Ramon J. Williams
Institution: University of Kentucky — College of Engineering
Date: Fall 2025

Overview

This report summarizes the outcomes of a simulated phishing campaign conducted using the open-source Gophish framework. The objective was to evaluate user awareness, analyze interaction metrics, and identify improvement opportunities in email security training and response behavior.

Methodology

The campaign consisted of three phases:

1. **Template Design** – Created authentic-looking phishing emails emulating standard business notifications and password resets.

2. **Target Distribution** – Sent 50 simulated phishing emails to volunteer participants within a controlled academic environment.

3. **Data Collection & Analysis** – Tracked opens, link clicks, and credential submissions through Gophish's dashboard and exported event logs for metric review.

Metric	Percentage	Description
Email Open Rate	**78%**	Users who viewed the email content.
Link Click Rate	**36%**	Users who clicked the embedded phishing link.
Credential Submission Rate	**10%**	Users who entered credentials into the mock login page.

Overall engagement indicated moderate awareness but highlighted vulnerabilities in link verification and sender trust assessment.

Observations

- Many participants failed to verify domain URLs before interacting.
- Urgency-based subject lines (e.g., “Action Required” or “Password Expiration Notice”) were most effective at triggering responses.
- Repeated exposure improved awareness — participants showed lower click rates after two rounds of training and follow-up testing.

Recommendations

1. **Regular Simulated Campaigns** — Reinforce awareness through periodic phishing exercises.
2. **Visual Cues Training** — Educate users on identifying domain mismatches, odd sender addresses, and security indicators.
3. **Report Button Integration** — Encourage quick reporting by embedding a “Report Phish” shortcut in email clients.
4. **Multi-Factor Authentication (MFA)** — Ensure secondary verification for all critical logins.

Conclusion

This simulation provided practical insights into user behavior and emphasized the value of consistent, data-driven awareness programs. By combining ongoing training, policy reinforcement, and secure authentication practices, organizations can effectively reduce their exposure to phishing-based threats.

Ramon J. Williams
Computer Science & Cybersecurity Student
University of Kentucky — Lexington, KY
ramonwilliams09@gmail.com
ramonwil.github.io