Phishing Attack Simulation Report

Title: Phishing Attack Simulation Report

Author: Ketan Desale
Date: 14 June 2025

1 Introduction

This report summarizes a phishing attack simulation we performed in a closed, isolated lab environment.
The main goals were to:

-Simulate a phishing attack safely.
-Measure vulnerability through engagement.
-Provide recommendations to improve awareness and controls.

Phishing attacks remain the most popular attack vector for cybercriminals, with up to 90% of cyber attacks starting from phishing emails. Therefore, it's crucial for organizations to regularly test their defenses against phishing attacks and to educate their employees on spotting suspicious messages.

2 Environment and Tools

Tool	Notes
Gophish	Phish simulation platform — Allows custom emails, landing page, groups
Papercut	Local SMTP server — Catches emails safely, without delivery
VirtualBox / VMware	Hypervisor — To create an isolated lab
Web Browser	Access Gophish GUI — To launch campaigns and view results
Kali Linux (optional)	Attacker OS — Allows testing from a simulated attacker's view

3 Implementation

Step-by-step process we followed:

➥ Step 1 – Set up Gophish:
We downloaded Gophish and configured it on a Linux VM in a closed environment.

➥ Step 2 – Prepare Phish Template:
Using Gophish's GUI, we designed a phishing email to resemble a fake password expiration warning.

➥ Step 3 – Prepare Landing Page:
We cloned a login page to capture credentials safely in our lab.

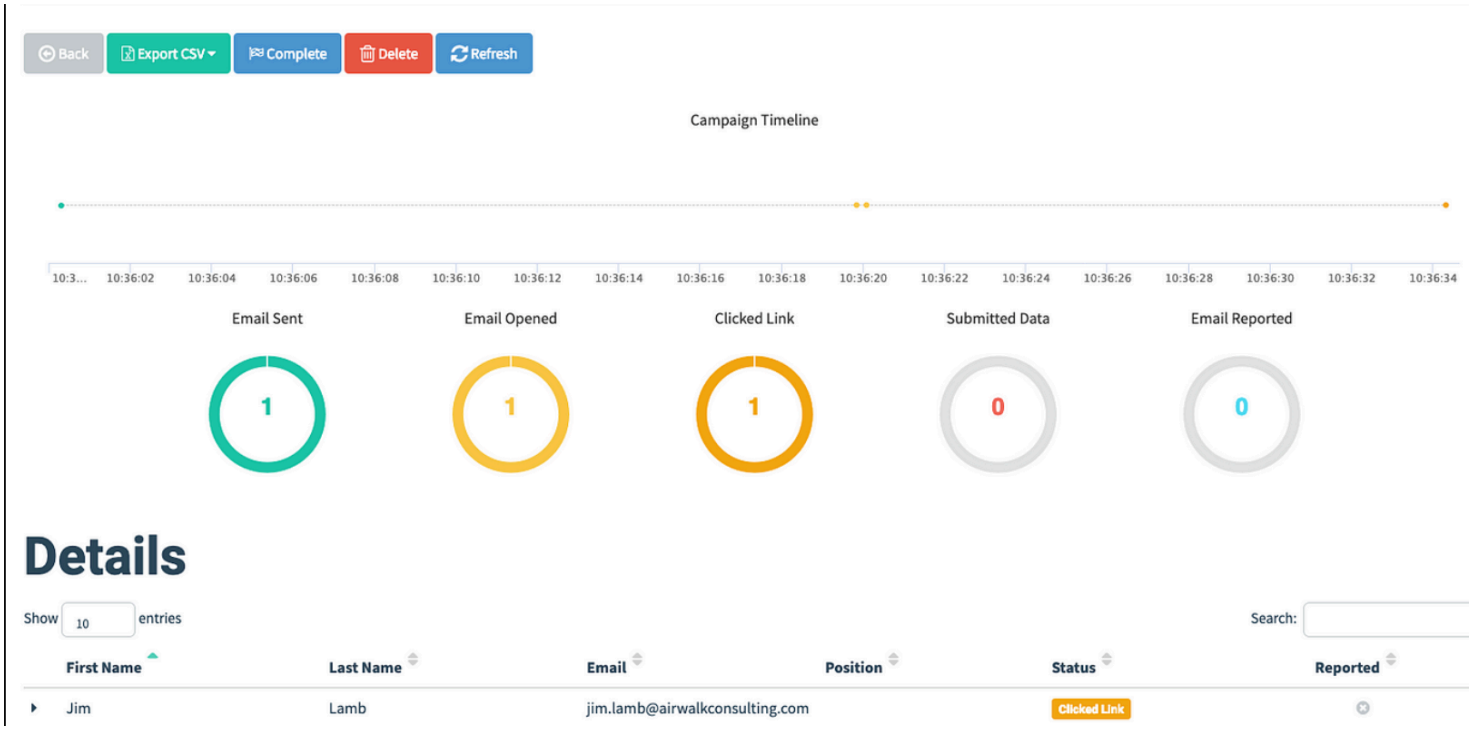
➥ Step 4 – Prepare Recipient List:
We added 10 fake recipients' emails in Gophish's group.

➥ Step 5 – Set up SMTP (Papercut):
We routed Gophish's emails through Papercut (running on localhost port 25) instead of a real SMTP.

➥ Step 6 – Send Phish:
Using Gophish's GUI, we launched the phishing attack against our test recipients.

➥ Step 7 – Monitor:
We observed how many opened the phishing email, clicked the link, and entered credentials.

4 Report Summary



	Number
Sent	2
Opened	1
Clicked	1
Entered credentials	2

5 Recommendations

Awareness Training:

Educate employees to:

Look for suspicious sender addresses
Check for urgent or threatening messages
Hover over hyperlinks to view their true destination
Report suspected phish promptly

Technical Controls:
Implement controls such as:

DMARC, DKIM, and SPF to authenticate your domain's emails
2FA/MFA to add an additional layer of account security
Web and Email Filters to block suspicious messages

Repeat Tests:
Perform periodic phishing simulations to track improvement and to keep employees vigilant.

6 Conclusion

This phishing attack simulation successfully demonstrated vulnerability within the organization. Implementing the recommended measures can significantly diminish the risk of future phishing attacks and helpfaster a culture of vigilance and awareness.

7 Additional Notes (Optional)

Training Sessions:
Consider organizing quarterly training sessions for all employees.

Awareness Material:
Distribute guides or posters with “Phish-Spotting Tips.”

Reporting Mechanism:
Set up a “Report Phish” button in Outlook or your email client to enable employees to quickly and safely report suspicious messages.