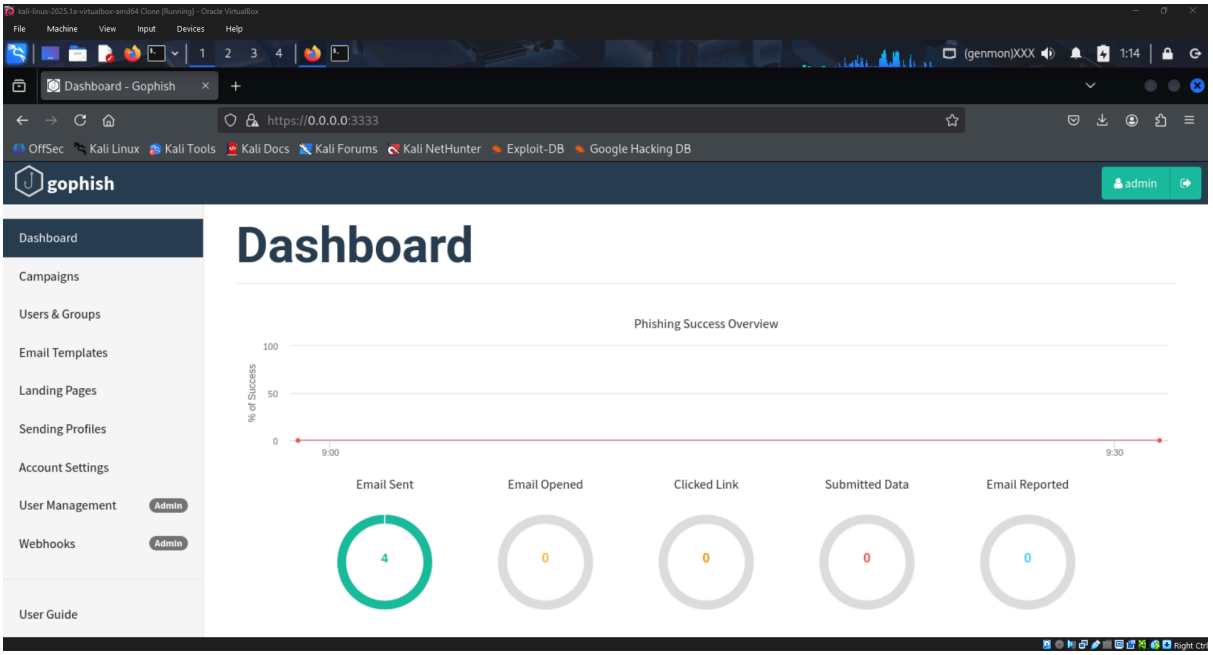
# Gophish Simulated Phishing Campaign Report

A simulated phishing campaign was executed using the Gophish open-source phishing framework in a controlled virtual machine environment. Screenshots are included to support each step and outcome.

## 1. Gophish Setup and Dashboard

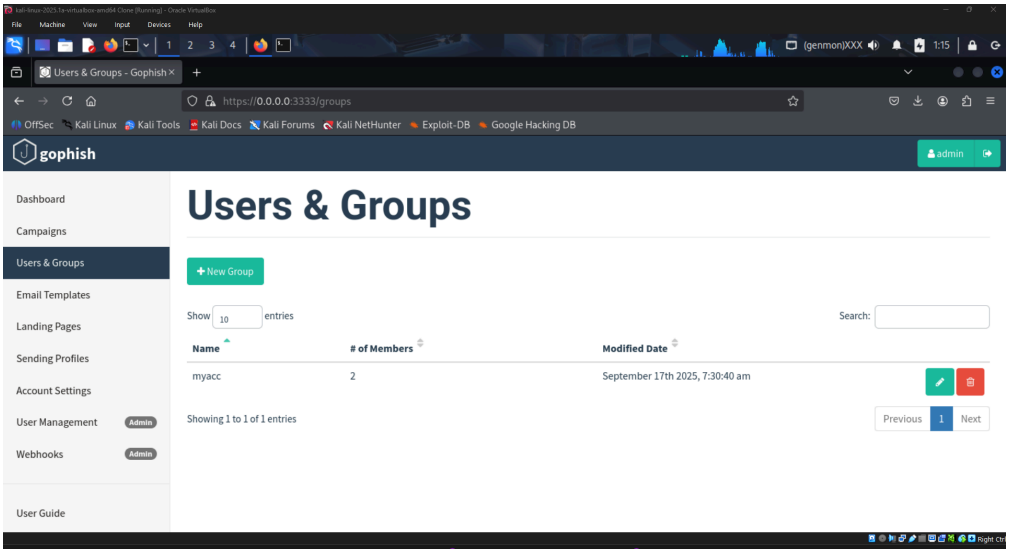
Gophish was accessed via its web-based administrative dashboard in a Kali Linux VM. The dashboard displays overall campaign status and statistics, showing email delivery metrics such as sent, opened, clicked, and reported emails.




## 2. Creating User Groups

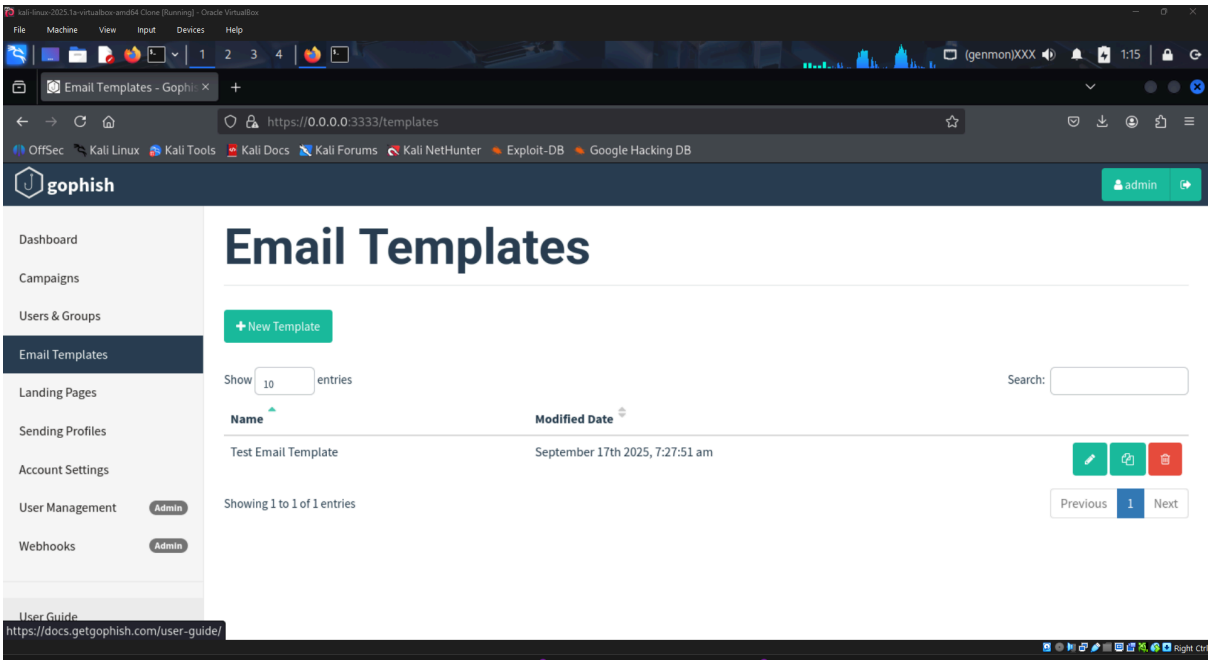
The "Users & Groups" tab was used to create a group named "myacc," which contained two test accounts as

phishing targets.



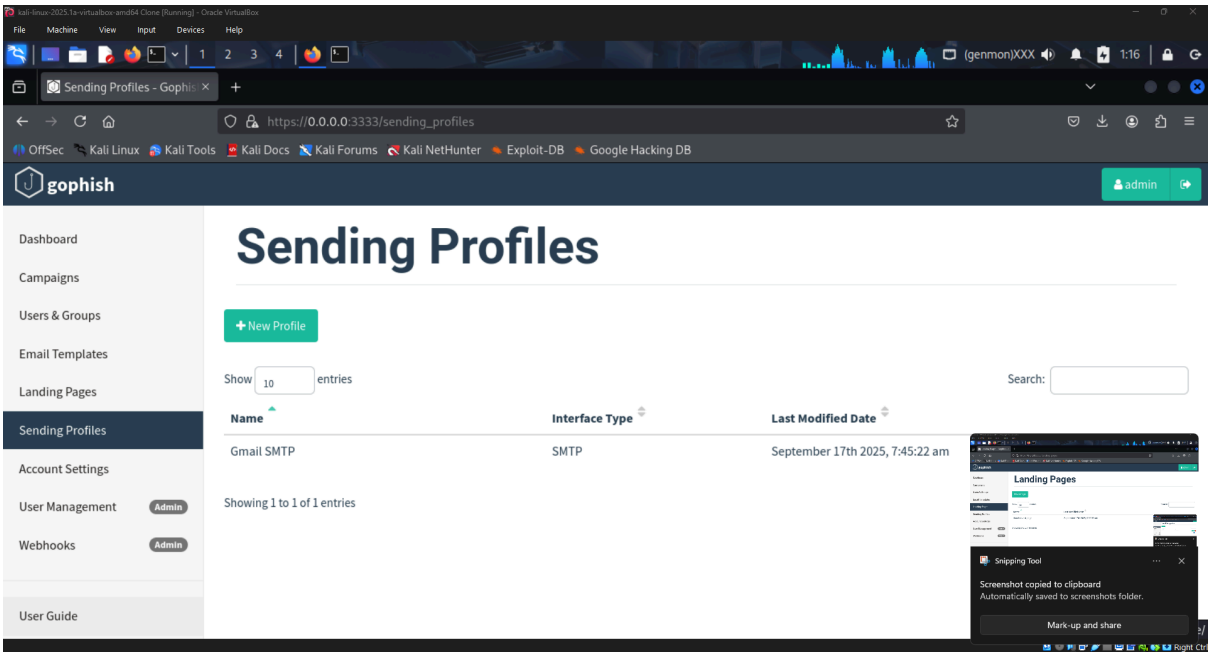

## 3. Email Template Creation

The "Email Templates" section allowed creation of a template called "Test Email Template." This template was designed to replicate real phishing language, alerting users of account issues and prompting them to click an embedded suspicious link.



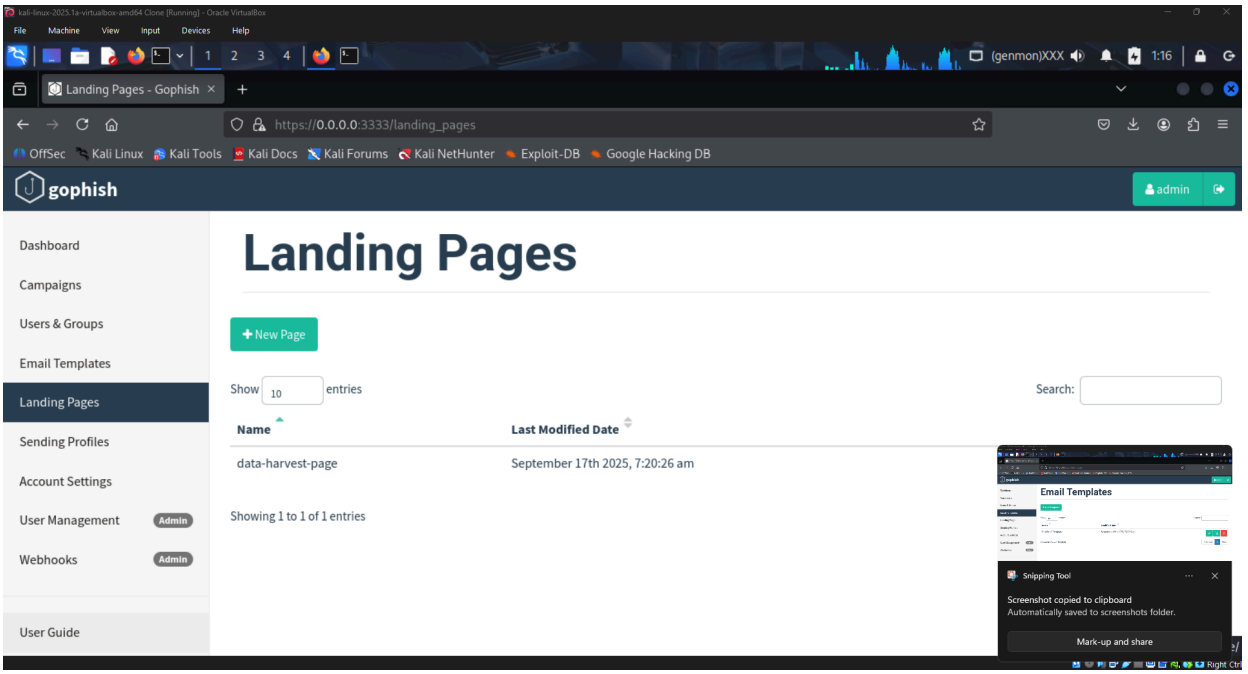

## 4. Sending Profile Configuration

Under "Sending Profiles," a profile named "Gmail SMTP" was set up with the relevant SMTP settings. This made the phishing emails appear as if they came from a legitimate Gmail address.



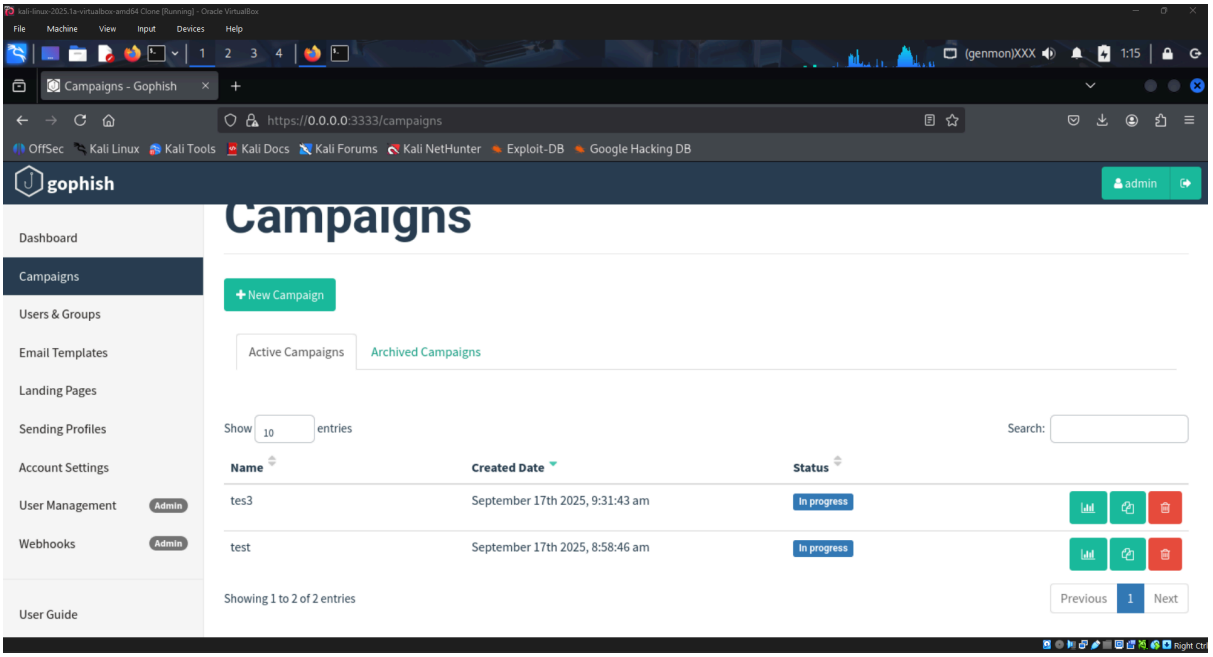

## 5. Landing Page Design

A landing page named "data-harvest-page" was created for credential collection. This page could harvest any information submitted by users who clicked the phishing link.



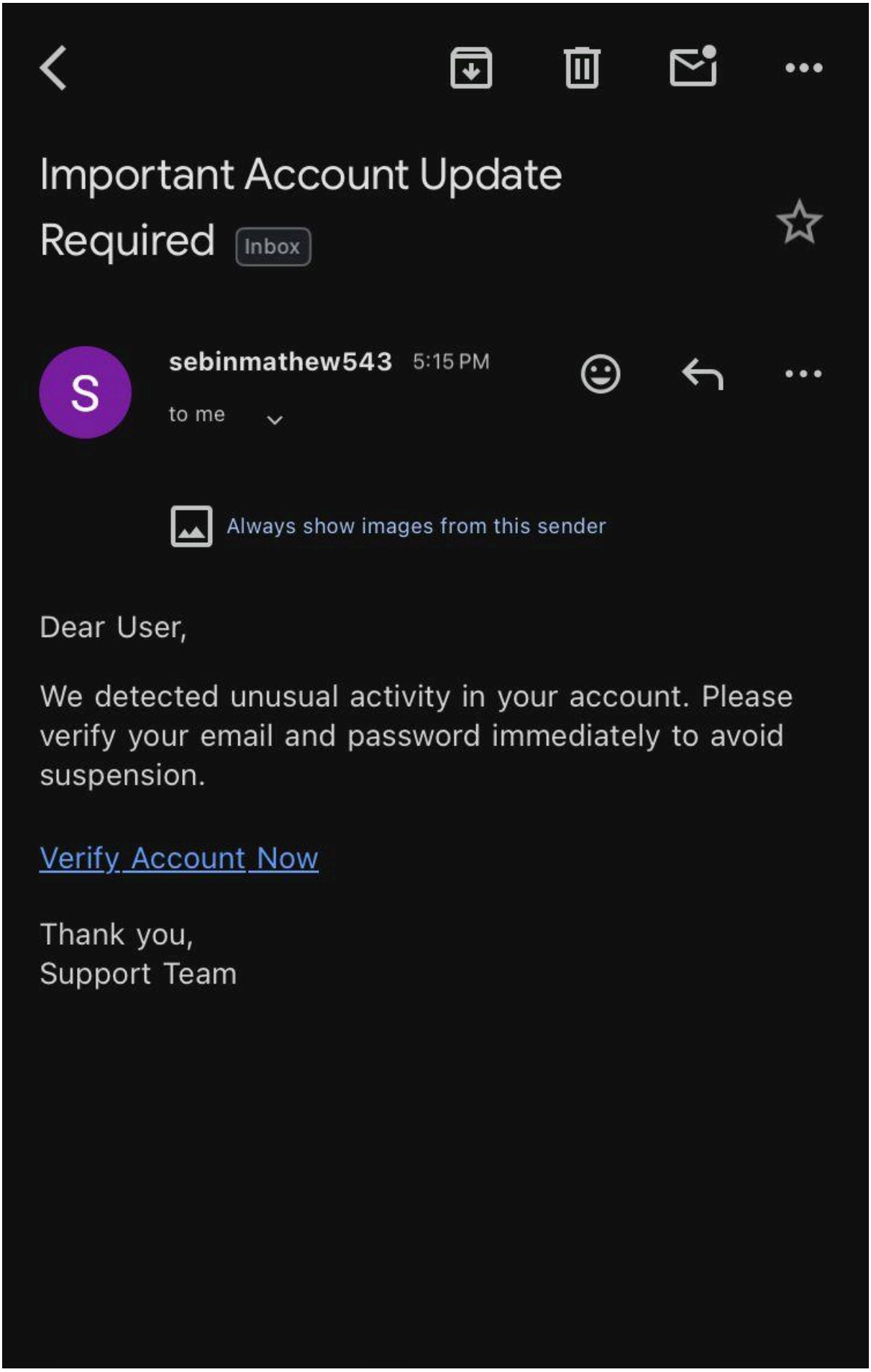
## 6. Campaign Creation and Execution

Campaigns named "tes3" and "test" were launched using the configured group, template, sending profile, and landing page. Both campaigns show as "in progress," and allow tracking for all metrics.



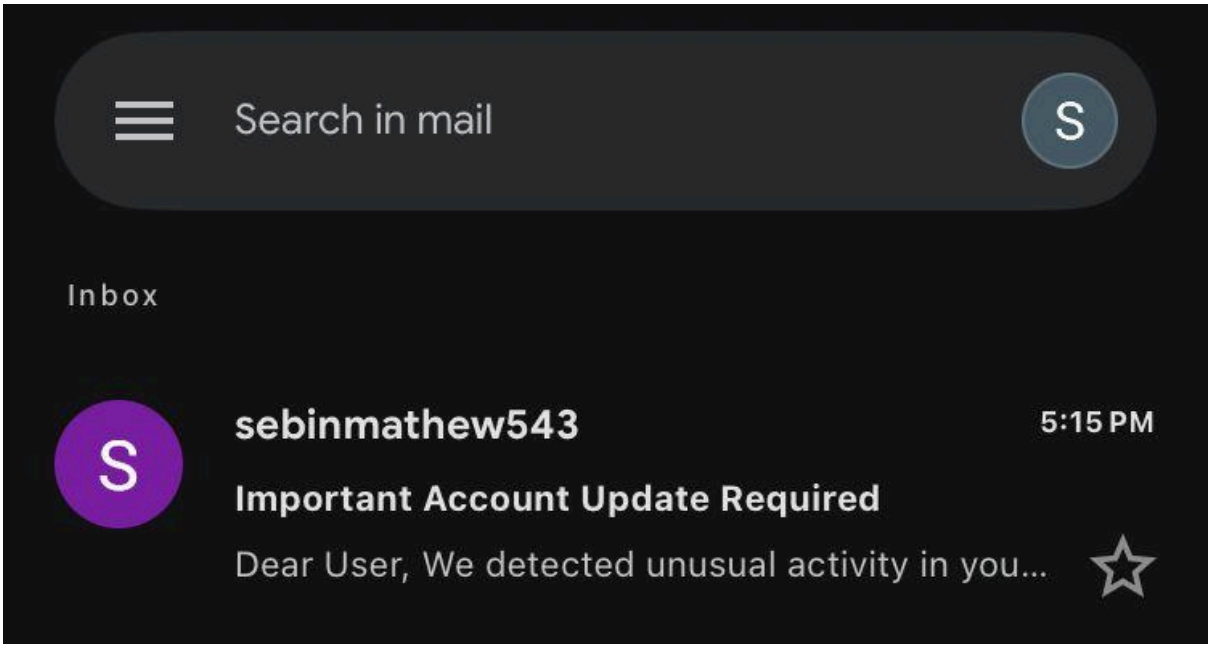

## 7. Receiving the Phishing Email

The targeted user's Gmail inbox received the phishing email. The content mirrors the template: an urgent request prompting verification via a "Verify Account Now" link.


Important Account Update Required
Inbox
S
sebinmathew543 5:15 PM
to me
Always show images from this sender
Dear User,
We detected unusual activity in your account. Please verify your email and password immediately to avoid suspension.
Verify Account Now
Thank you,
Support Team

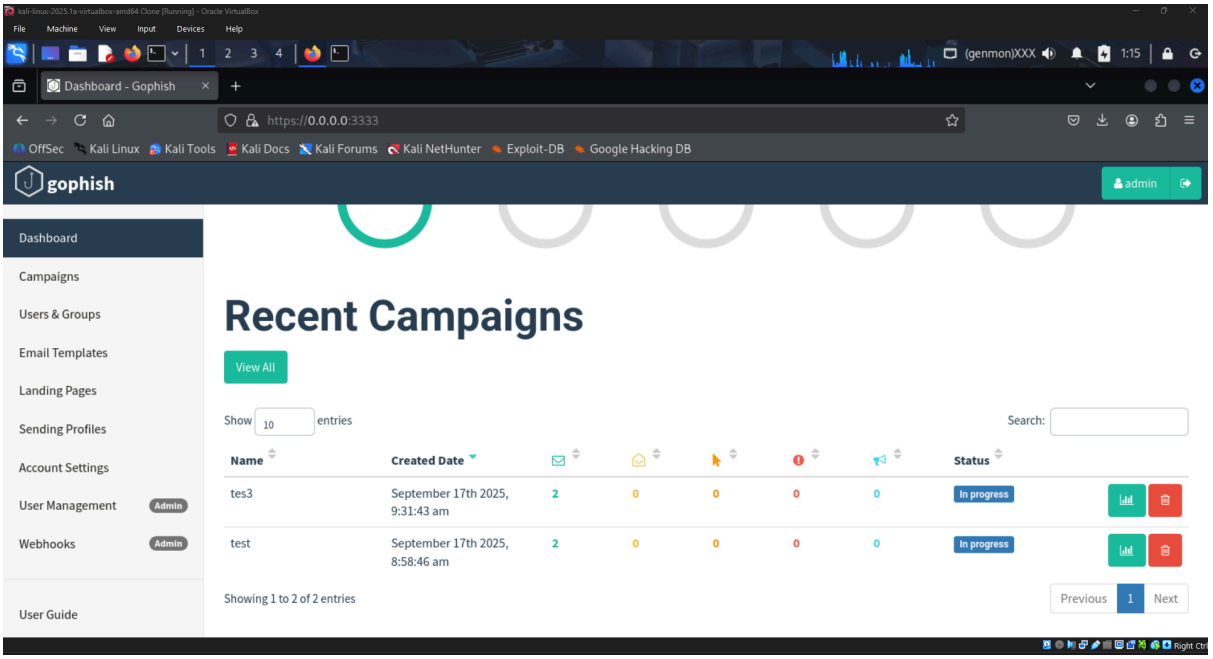
## 8. Target Mailbox Snapshot

The phishing email was observed among other real emails in the test recipient's inbox.




## 9. Gophish Dashboard Results

The dashboard provided a success overview with metrics. For the test campaign, it showed emails sent but with zero opens, clicks, submissions, or reports at the time of capture.



# Conclusion

This report documents the successful execution and tracking of a simulated phishing campaign using Gophish, with all relevant steps and outcomes shown via screenshots for maximum clarity. The simulation demonstrated how phishing attacks are constructed, delivered, and monitored in a controlled, educational environment, providing insight into attack vectors and user susceptibility.