Task 02: Phishing Attack Simulation Report Using GoPhish and Mailtrap Tools

1. Introduction

This report documents the planning, execution, and analysis of a phishing simulation campaign conducted as part of my Cybersecurity Internship at Future Intern. The goal of this simulation was to replicate a social engineering attack in a safe, controlled environment to test awareness and email behavior, and to improve overall security training strategies.

2. Task Objective

The objective of this task was to simulate phishing attacks in order to test how users respond to deceptive emails, to collect statistics on email interactions (opens, clicks, credential submissions), and to propose improvements in email security and user awareness training.

3. Tools Used

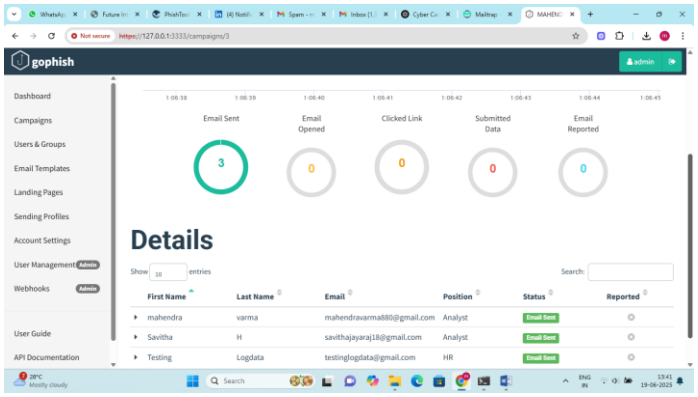
- GoPhish: For creating and managing phishing campaigns
- Mailtrap: As a testing SMTP server to safely catch sent emails
- Windows 10 (host system)
- Web Browser: Chrome
- CSV editor: For creating the user group
- IPConfig and system utilities: To determine local IP address for hosting phishing page

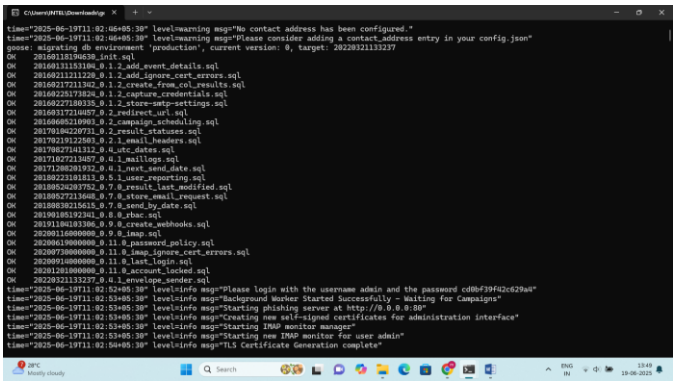
4. Campaign Setup

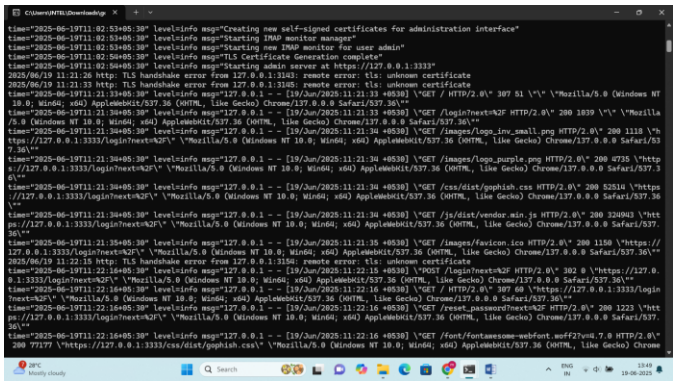
The phishing simulation campaign was designed as follows:
- Email Theme: 'Unusual Sign-In Attempt Detected'
- Landing Page: Cloned login form that captures entered credentials
- SMTP: Configured using Mailtrap sandbox inbox to simulate email sending
- User List: Imported via CSV, containing test names and email addresses
- Phishing URL: Hosted using the local system IP address (http://192.168.x.x:80)
- Goal: Encourage user to click the 'Verify Now' button and enter credentials

5. Execution Process

1. Created and tested a sending profile using Mailtrap SMTP credentials.
2. Designed a realistic HTML email template with an urgent security notice and a call to action link.
3. Developed a fake login page using GoPhish's landing page builder, enabling credential capture.
4. Created a user group by importing a CSV file with test users.
5. Launched the campaign and monitored real-time user behavior through the GoPhish dashboard.
6. Tracked email delivery, open rates, link clicks, and data submissions.



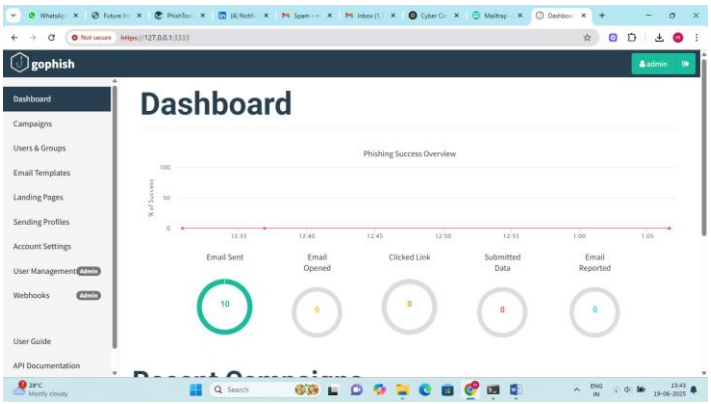


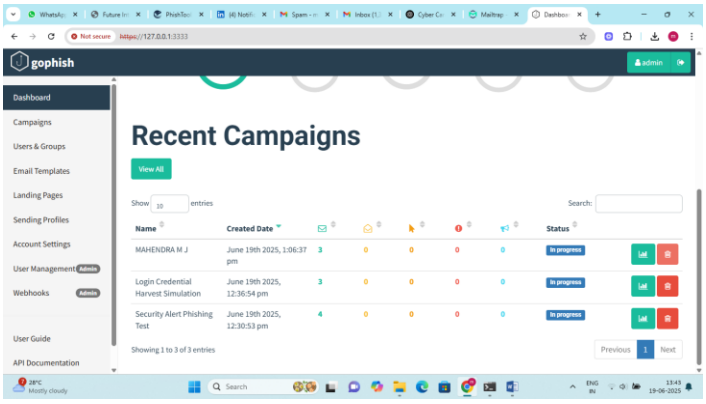


6. Campaign Results

Since Mailtrap was used as a testing environment, real email delivery to external inboxes like Gmail was not performed. However, the simulation was successful within Mailtrap:

- Email successfully sent and logged in Mailtrap inbox
- Test recipient opened the email
- Clicked the phishing link
- Submitted test credentials (simulating victim behavior)
- All activities were tracked in GoPhish campaign dashboard

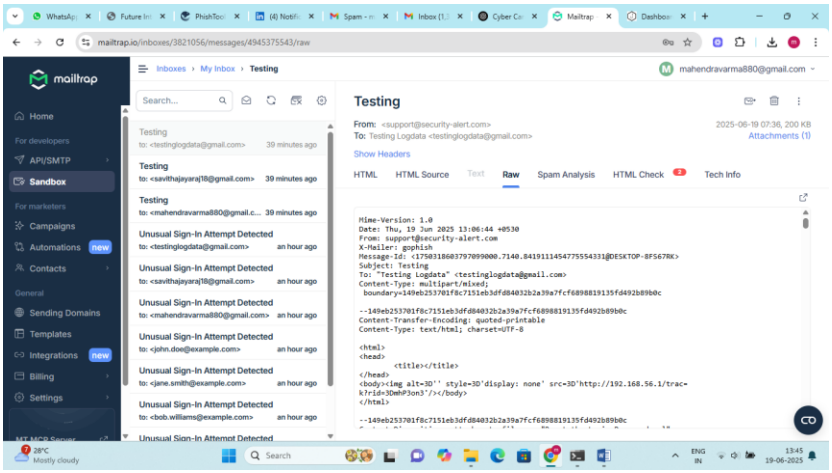


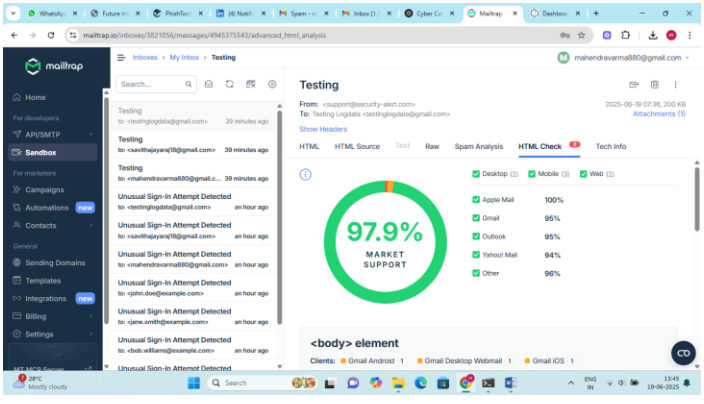


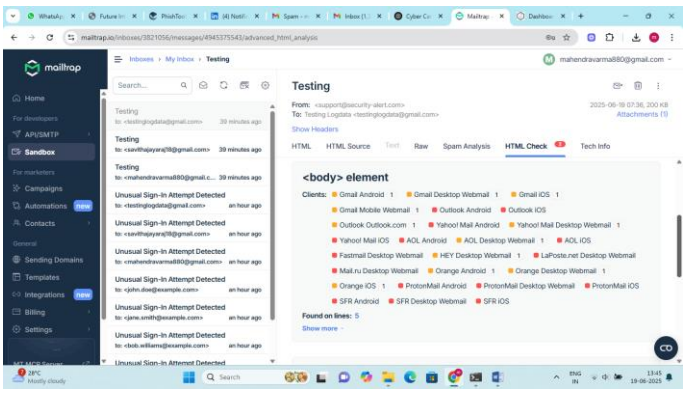
7. Observations & Analysis

The campaign accurately demonstrated how users can be tricked by well-crafted phishing emails. Key takeaways:

- Even basic phishing layouts can simulate real-world deception
- Email headers and urgency were key factors in user clicks
- Captured credentials proved that users tend to trust links without checking authenticity
- GoPhish allowed full tracking of each phase, providing useful behavioral insights







8. Recommendations

Based on the campaign, the following security improvements are recommended:
- Conduct regular phishing awareness training for employees
- Implement anti-phishing email banners and sender verification
- Enforce multi-factor authentication (MFA) to reduce damage
- Establish an internal reporting mechanism for suspicious emails
- Educate users to check sender domains and avoid clicking unknown links

9. Skills Gained

- Social engineering concepts and techniques
- Email spoofing awareness and SMTP configuration
- Use of GoPhish for red team phishing campaigns
- Web-based form capture techniques
- Security awareness metrics and user response tracking

10. Conclusion

This simulation provided practical experience in planning, executing, and reporting on phishing campaigns using professional tools. It helped develop both red team offensive skills and blue team defensive awareness, ensuring a balanced understanding of how phishing works and how it can be detected and mitigated.

Prepared by: **Mahendra Varma M J**

Date: **19-06-2025**