Phishing Simulation Report – Task 2 (Cybersecurity Internship)

# 1. Overview

Intern Name: [Your Name]  
Track: Cyber Security (Track Code: CS)  
Task: Social Engineering & Phishing Simulation  
Tools Used: Gophish, Gmail SMTP, HTML (Instagram Clone)  
Target: Self (Test Account - nanadans59@gmail.com)

# 2. Objective

Simulate a phishing attack to evaluate user awareness and test the effectiveness of phishing emails using Gophish.

# 3. Attack Vector

Type: Email Phishing (Impersonation of Instagram Security Team)  
Email Subject: Important Security Check  
Landing Page: Fake Instagram Login (HTML clone)  
Link URL: http://192.168.30.1

# 4. Methodology

|  |  |
| --- | --- |
| Step | Action |
| 1 | Set up Gophish on Windows |
| 2 | Configured SMTP using Gmail App Password |
| 3 | Created phishing email template using minimal HTML |
| 4 | Imported Instagram clone landing page with modified <form action='/post'> |
| 5 | Created campaign with target email: nanadans59@gmail.com |
| 6 | Monitored results through the Gophish dashboard |

# 5. Results Summary

|  |  |  |  |
| --- | --- | --- | --- |
| Target Email | Email Delivered | Link Clicked | Credentials Submitted |
| nanadans59@gmail.com | Yes | Yes | Yes |

# 6. Visual Evidence

- Screenshot: Received phishing email in Gmail  
- Screenshot: Instagram-style fake login page  
- Screenshot: Gophish campaign dashboard showing activity

# 7. Recommendations

- Conduct recurring phishing awareness training  
- Teach users to hover over links to verify authenticity  
- Implement multi-factor authentication (MFA) on all accounts  
- Use mail gateways that detect spoofed domains

# 8. Conclusion

This phishing simulation successfully demonstrated how easy it is to mimic legitimate platforms and how critical user awareness and strong email security are in defending against such attacks.