Phishing Simulation Project - Conclusion Report

# 1. Objective

The main aim of the project was to simulate phishing attacks in a controlled environment to study user awareness, response, and vulnerability. Tools like Gophish were used to design phishing campaigns, send emails, and track results.

# 2. Results

Based on the simulation carried out, the following results were observed:

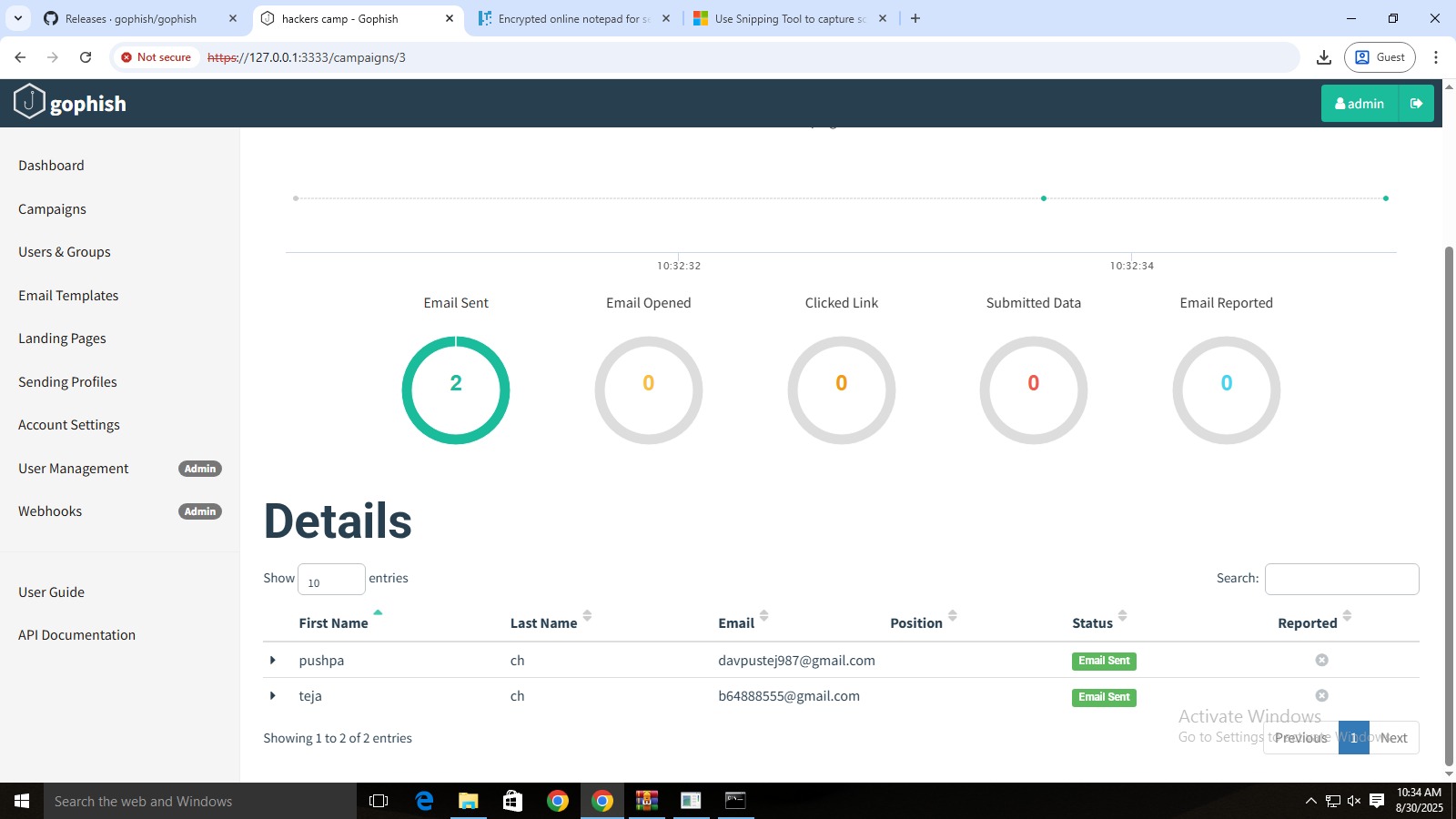


Figure: Result from result 1.jpg

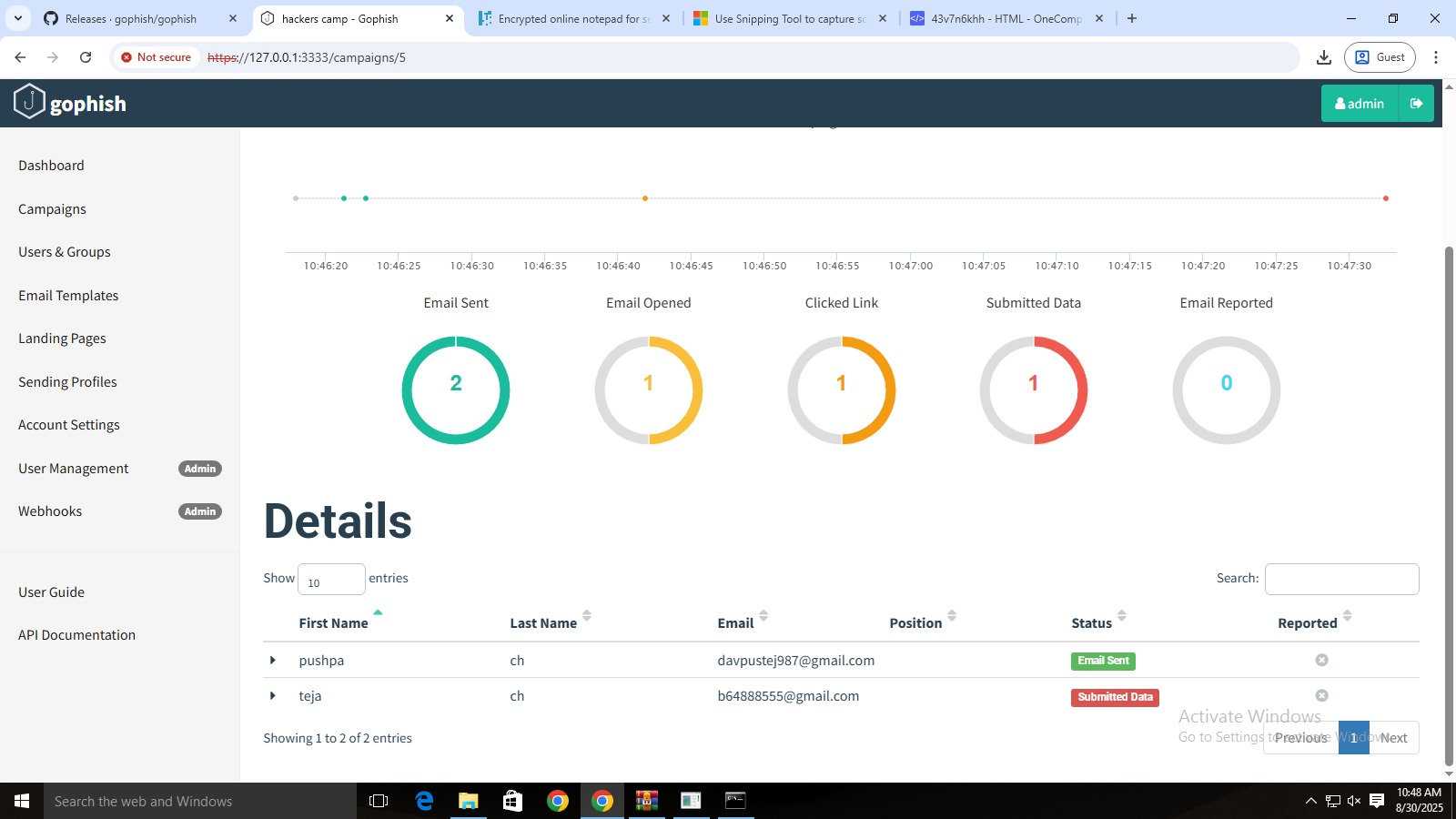


Figure: Result from result2.jpg

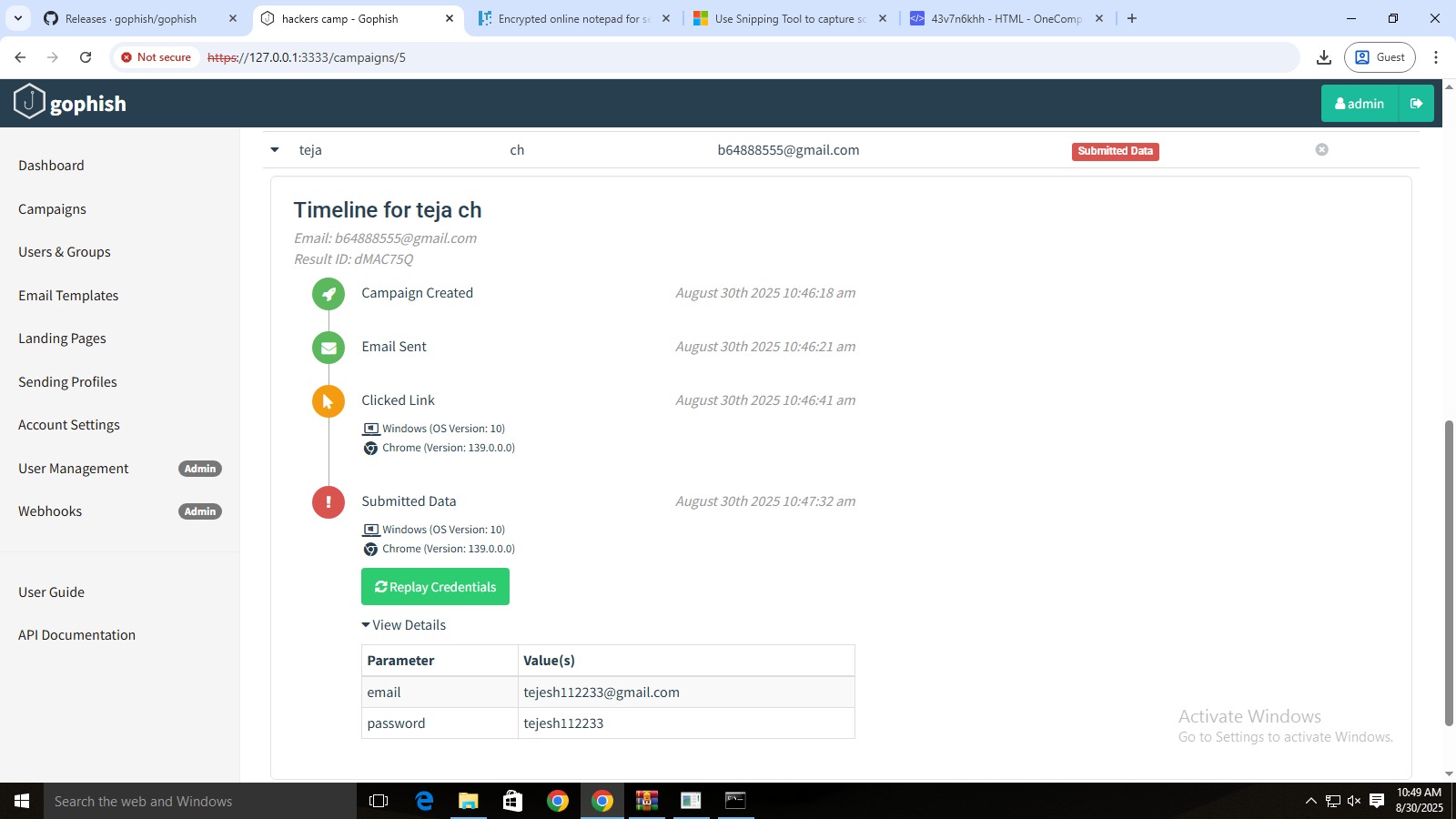


Figure: Result from crediational1.jpg

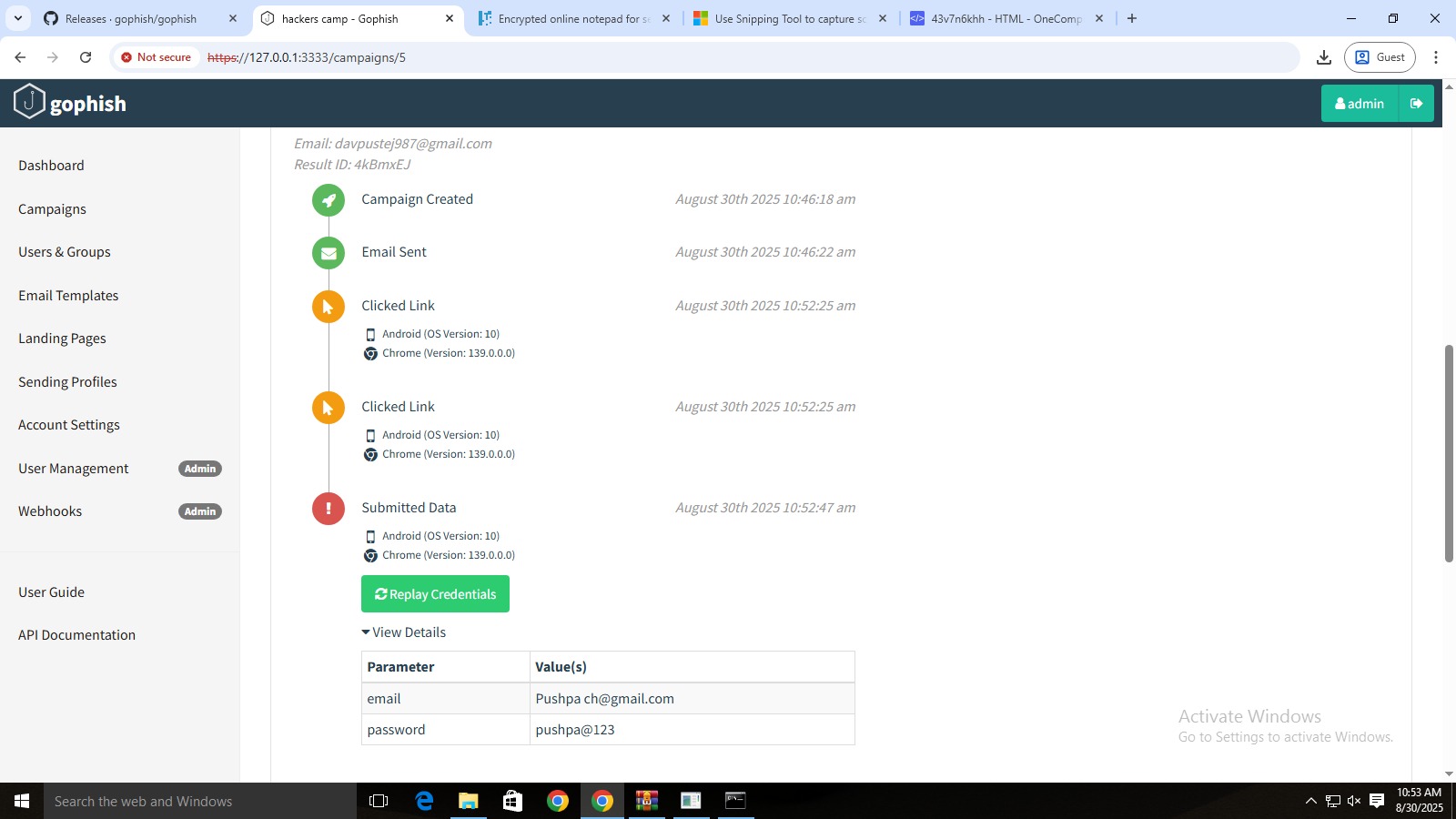


Figure: Result from credentional2.jpg

- Emails Sent: 2  
- Emails Opened: 1  
- Links Clicked: 1  
- Credentials Submitted: 2 (both users submitted credentials)  
  
This indicates that phishing attempts can be highly successful if users are not aware or cautious.

# 3. Key Observations

- Even with a small sample group (2 users), 100% submitted credentials.  
- Users did not report the phishing attempt, showing low awareness.  
- The simulation highlights the risk factor of human error in cybersecurity.

# 4. Conclusion

The project demonstrates that phishing remains one of the most effective cyberattacks due to human negligence. Without proper training, users can easily fall victim to phishing campaigns. Such simulations are valuable to test awareness and design cybersecurity training programs.

# 5. Future Scope

- Expand the test to a larger group.  
- Introduce different phishing templates (banking, social media, office mail, etc.).  
- Integrate awareness training after the simulation.  
- Automate report generation to present statistics clearly.