TASK 2: PHISHING AWARENESS TRAINING

What is phishing attack?

Phishing is a social engineering tactic where attackers deceive individuals into performing actions. Phishing attacks remain one of the most prevalent and damaging forms of cybercrime. These deceptive tactics involve cybercriminals impersonating trusted digital platforms such as developer tools, cloud services, or collaboration sites to trick users into revealing sensitive information.

This project aims to understand the mechanics of phishing by simulating a realistic email phishing campaign, focused on the widely used software development platform GitHub. The phishing simulation replicates a standard GitHub account alert email, designed to lure recipients into a fake login page (github.au) crafted to harvest credentials.

Through this controlled and ethical simulation, I examine user behavior, identify psychological manipulation techniques, evaluate attack success metrics, and offer mitigation strategies for developers, security teams, and organizations.

Common objectives include:

• Credential harvesting (e.g., GitHub login details)

**Attack Simulation**

In this simulation, a fake GitHub email was created, alerting users to unusual login activity and urging them to secure their account by logging in. The email contained authentic GitHub branding and led to a cloned login page hosted at github.au.

Execution:

• An email template was created, replicating official GitHub alerts in tone, style, and formatting.

• The phishing message warned about suspicious login attempts and directed users to “Secure Your Account.”

• The login page was cloned to mimic github.com and modified to send submitted credentials to a backend logger.

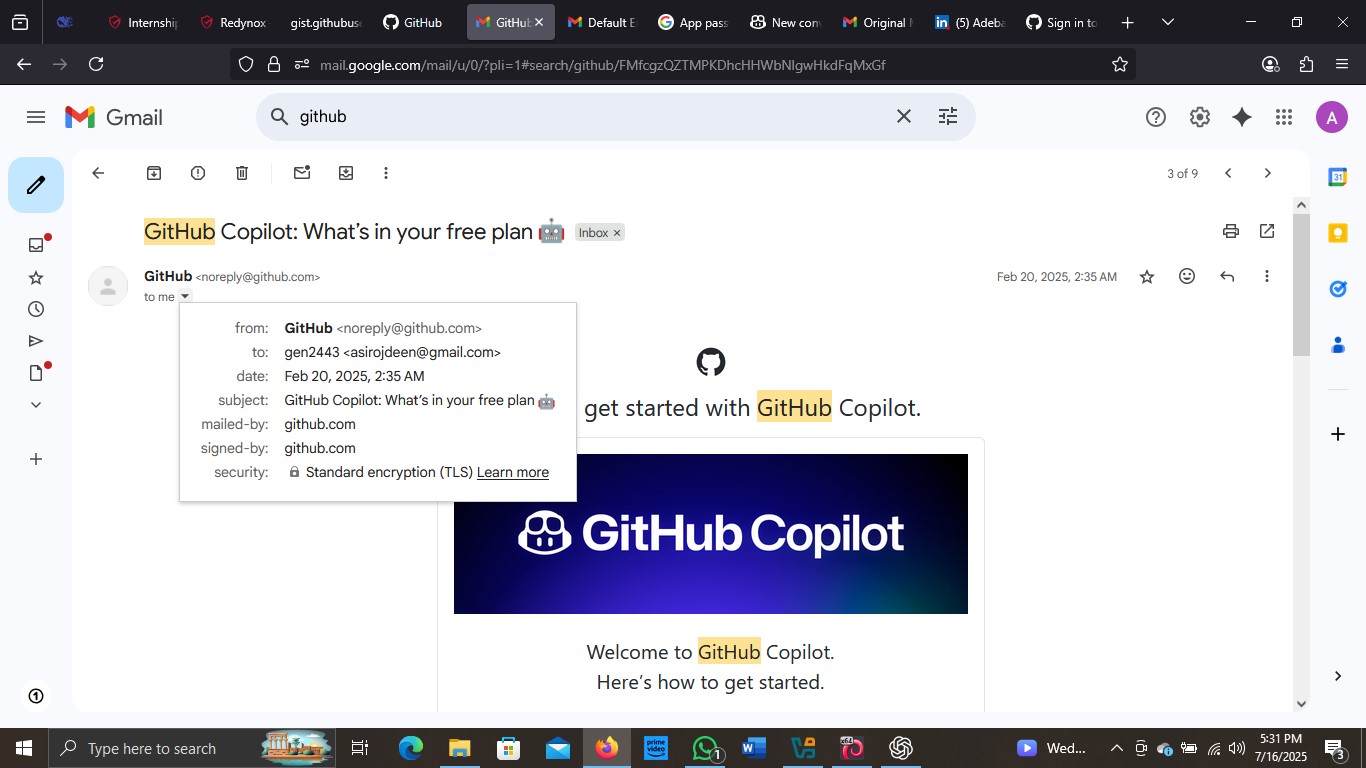
**Key Indicators of a Phishing Email**

• Domain mismatch: (github.au@gmail.com vs noreply@github.com

• Urgency or fear: (“We detected unauthorized login attempts on your account”)

• Email metadata anomalies: Emails sent via gmail.com instead of GitHub’s mail servers {Github.com}

Email Sample Comparison





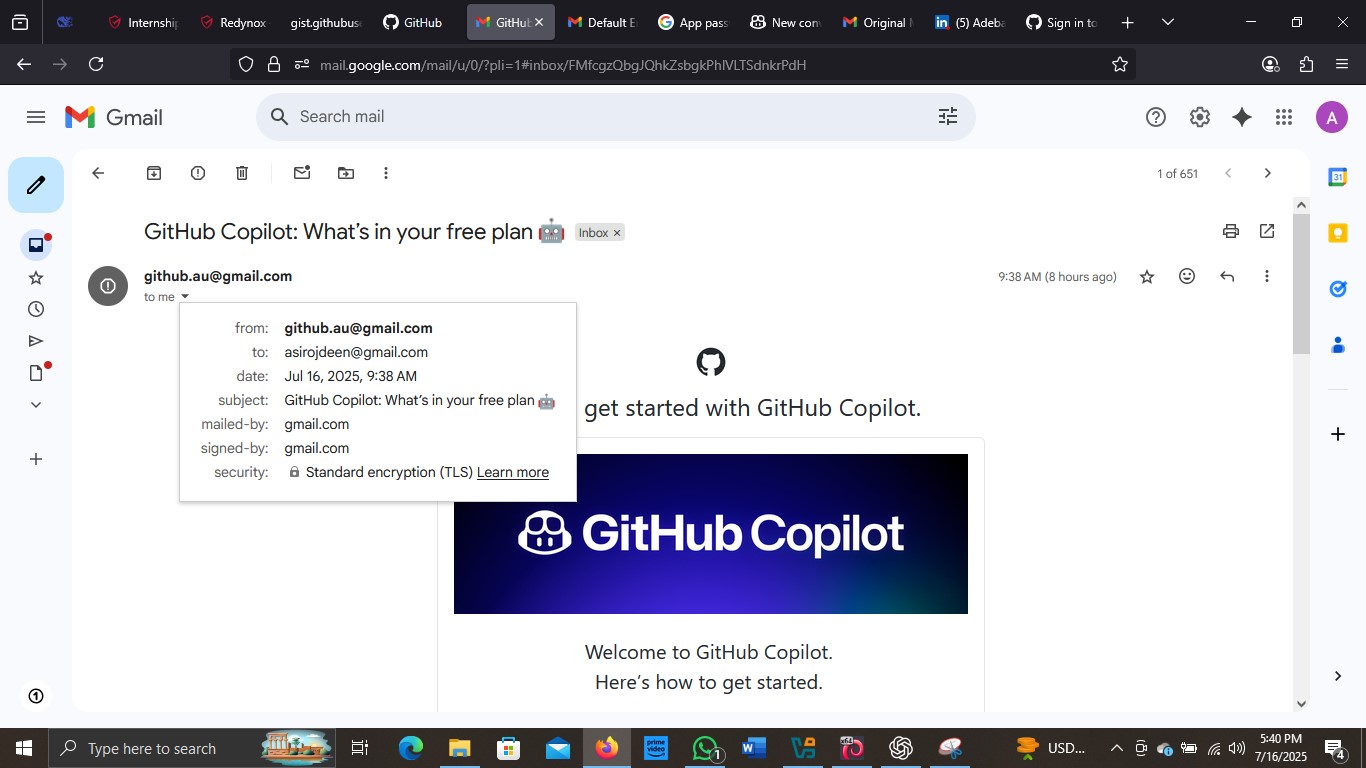
**Original Email:**

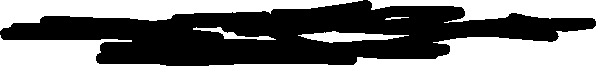
Sent from: noreply@github.com

Signed by: github.com

Secure headers and domain alignment

**Cloned Email:**





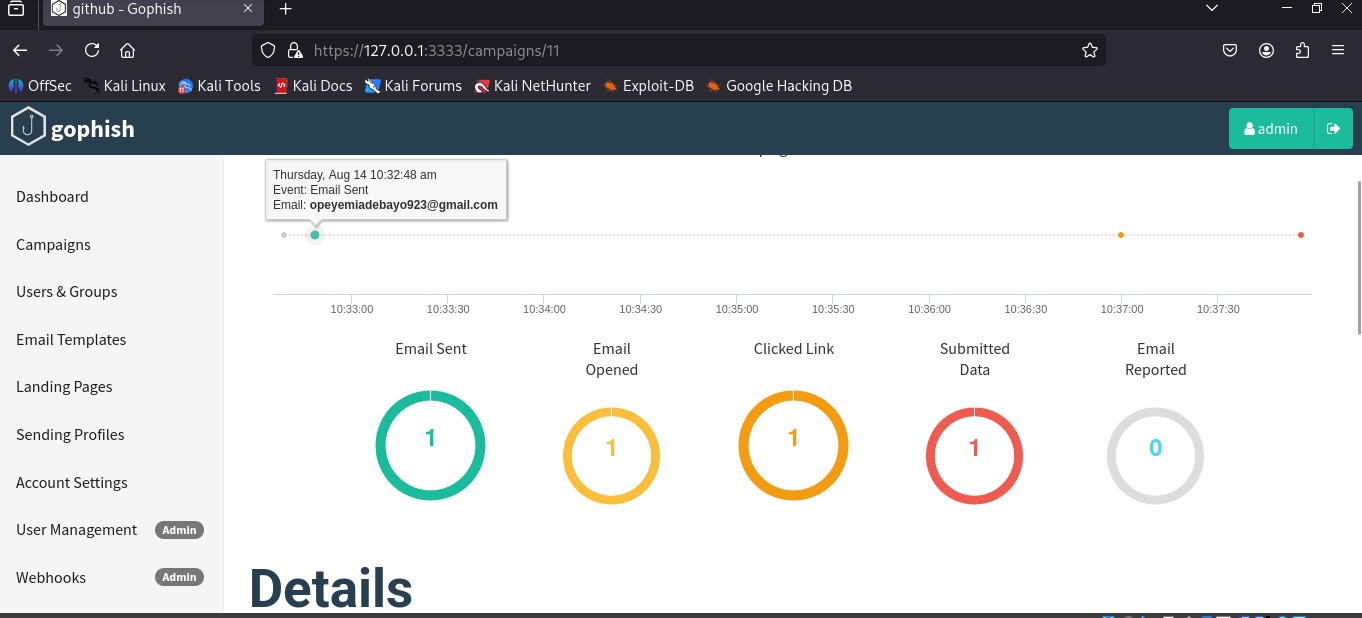
Sent from: github.au@gmail.com

Signed by: gmail.com

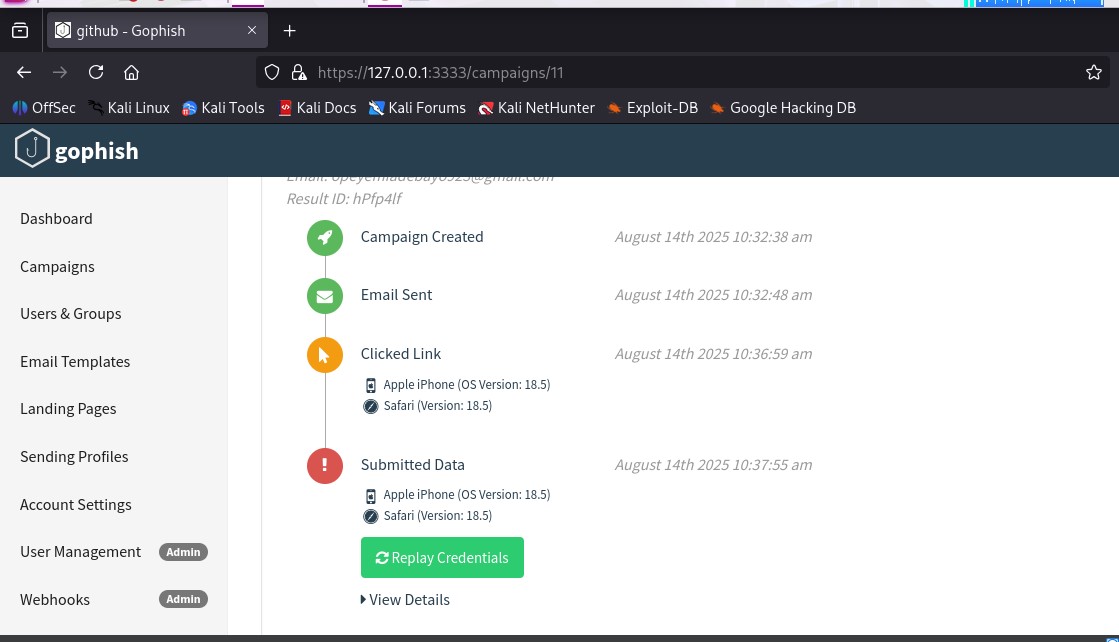
No domain alignment, suspicious sender, and no SPF/DKIM records

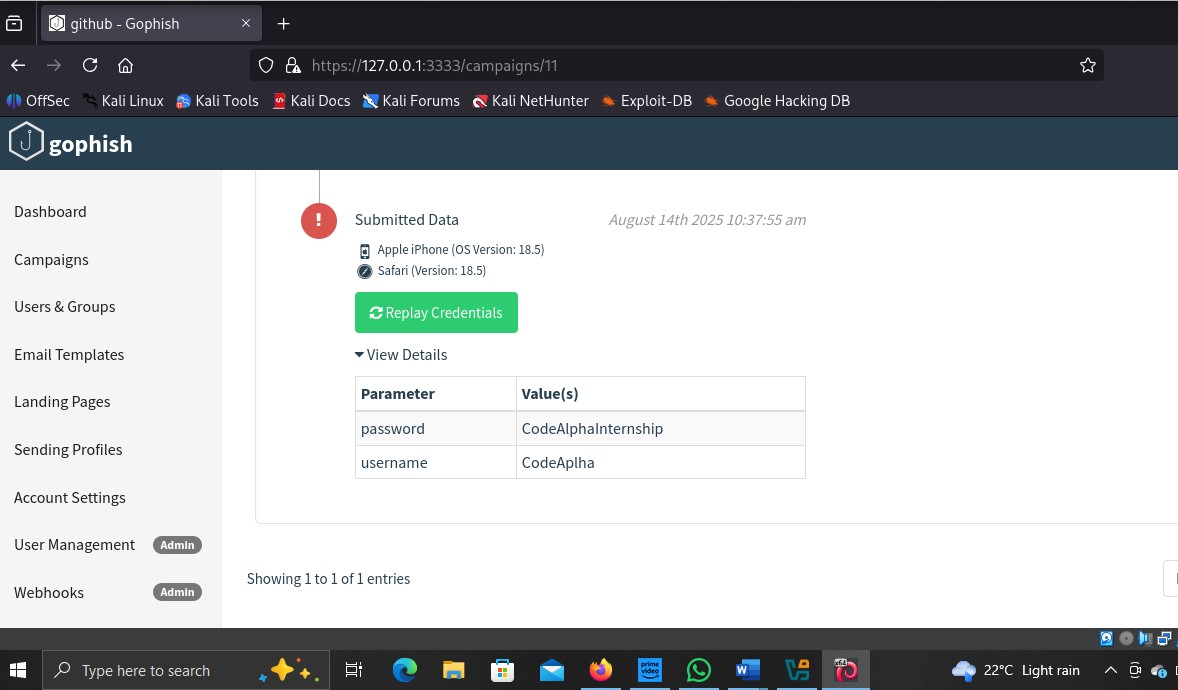
**RESULT OF THE ATTACK**

Attacker’s information









Mitigation Strategies

• Always verify the email sender and domain carefully

• Check links before clicking inspect the real URL

• Enable 2FA (Two-Factor Authentication) on GitHub

• Use GitHub’s security features like verified sessions and audit logs

• Report suspicious messages to abuse@github.com

Conclusion

Phishing attacks have become increasingly sophisticated, targeting even technical communities such as software developers and DevOps engineers. This simulation using a GitHub clone (github.au) demonstrates how attackers can exploit branding, urgency, and human psychology to deceive even experienced users.

By studying these tactics, we gain insight into how to build resilient defenses, promote user awareness, and encourage a security-first mindset across technical ecosystems.

**DISCLAIMER: This project is strictly for educational purposes only. No real users were targeted or harmed. All data collection occurred in a closed testing environment for cybersecurity learning.**

**All data collection was done in a controlled environment for research and educational purposes only.**