Task 2: Social Engineering & Phishing Simulation

# Phishing Campaign Report:

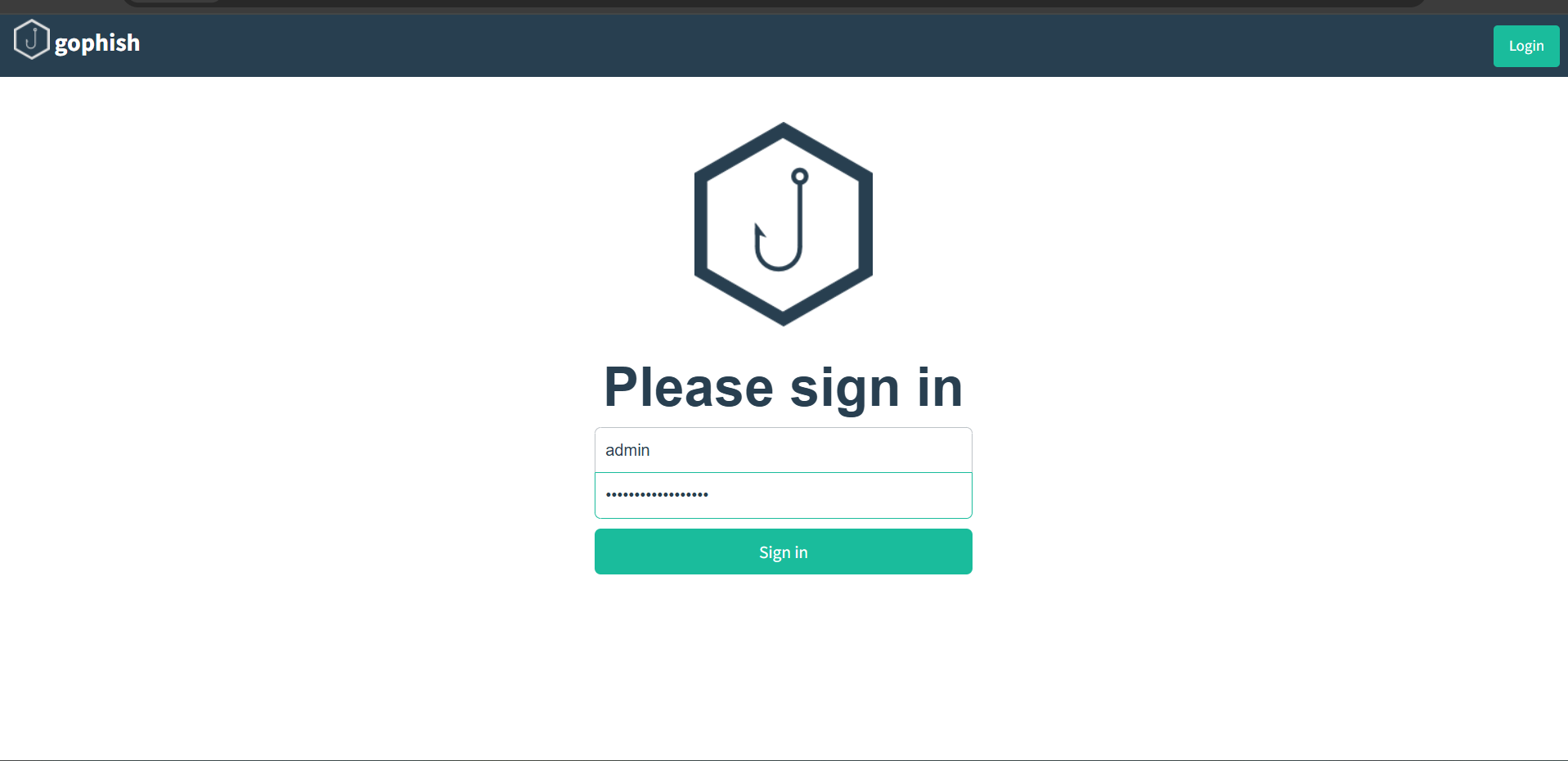
## Objective:

The goal of this phishing campaign was to test the awareness of recipients regarding potential phishing attacks and to evaluate their responses. This will contribute to the development of effective security training programs for employees, focusing on recognizing suspicious emails and protecting against social engineering tactics.

## Phishing Campaign Setup:

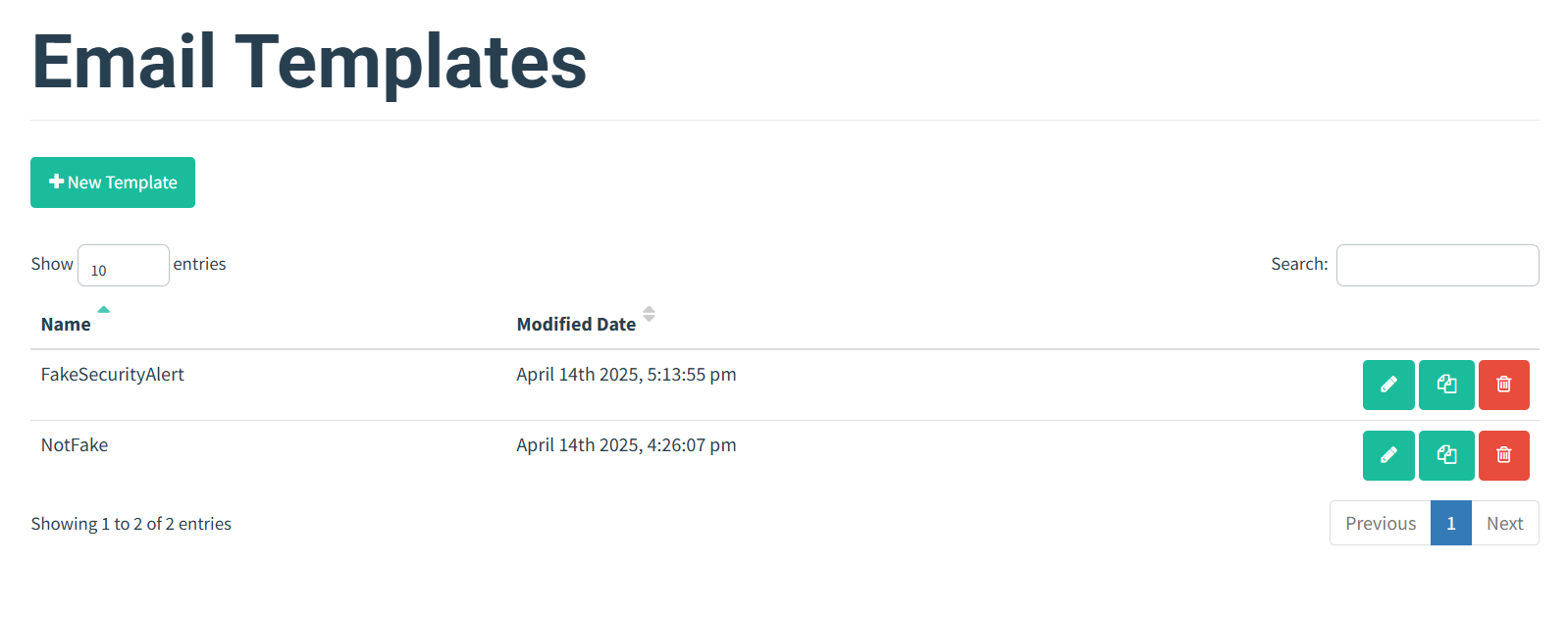
#### Tools Used:

* **Gophish**: A framework used for creating and managing phishing campaigns.
* **SET (Social Engineering Toolkit)**: Optional tool for simulating social engineering attacks, though Gophish was primarily used.



#### Email Templates Used:

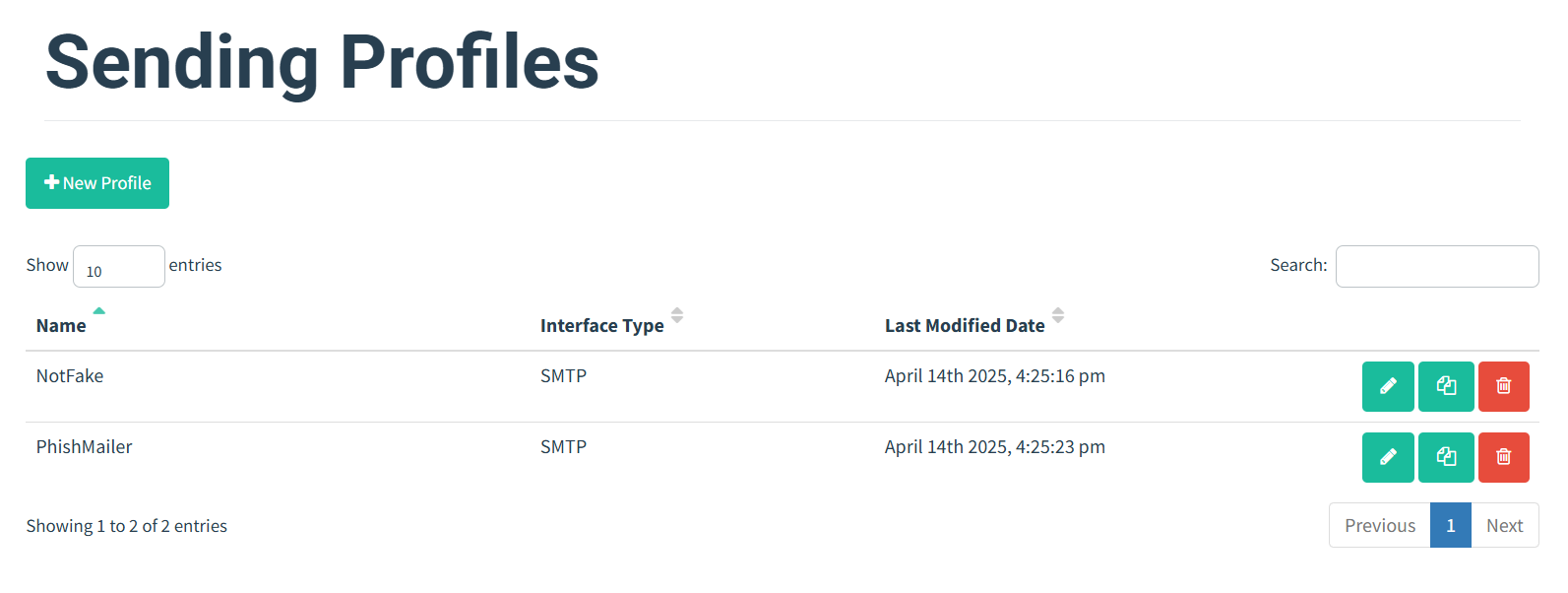
* **Template 1**: An email posing as a representative from a cybercrime portal, instructing recipients to check all their folders. (NotFake template)
* **Template 2**: An email claiming that unusual activity had been detected in the recipient's account, asking them to click a link to verify their login. This email was sent from an address designed to look suspicious ([cybercrime.analysts1930@gmail.com](mailto:cybercrime.analysts1930@gmail.com)). (FakeSecurityAlert template)



#### Sending Profiles:

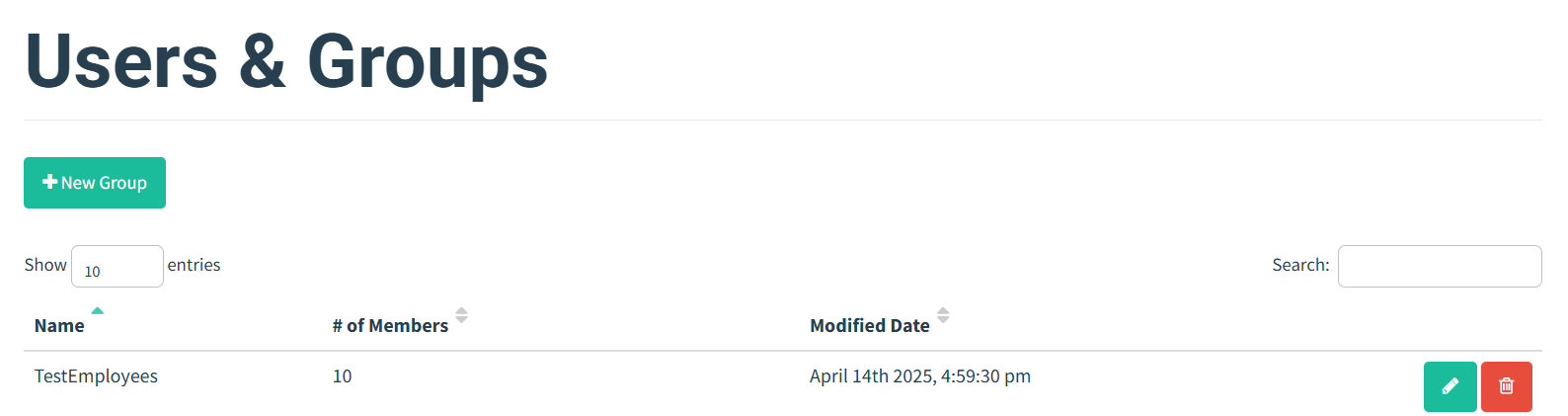
Two distinct sending profiles were generated to simulate realistic phishing campaigns:

* **Profile 1**: A representative of a cybercrime portal.
* **Profile 2**: A fake analyst from a cybercrime detection service. (PhishMailer)



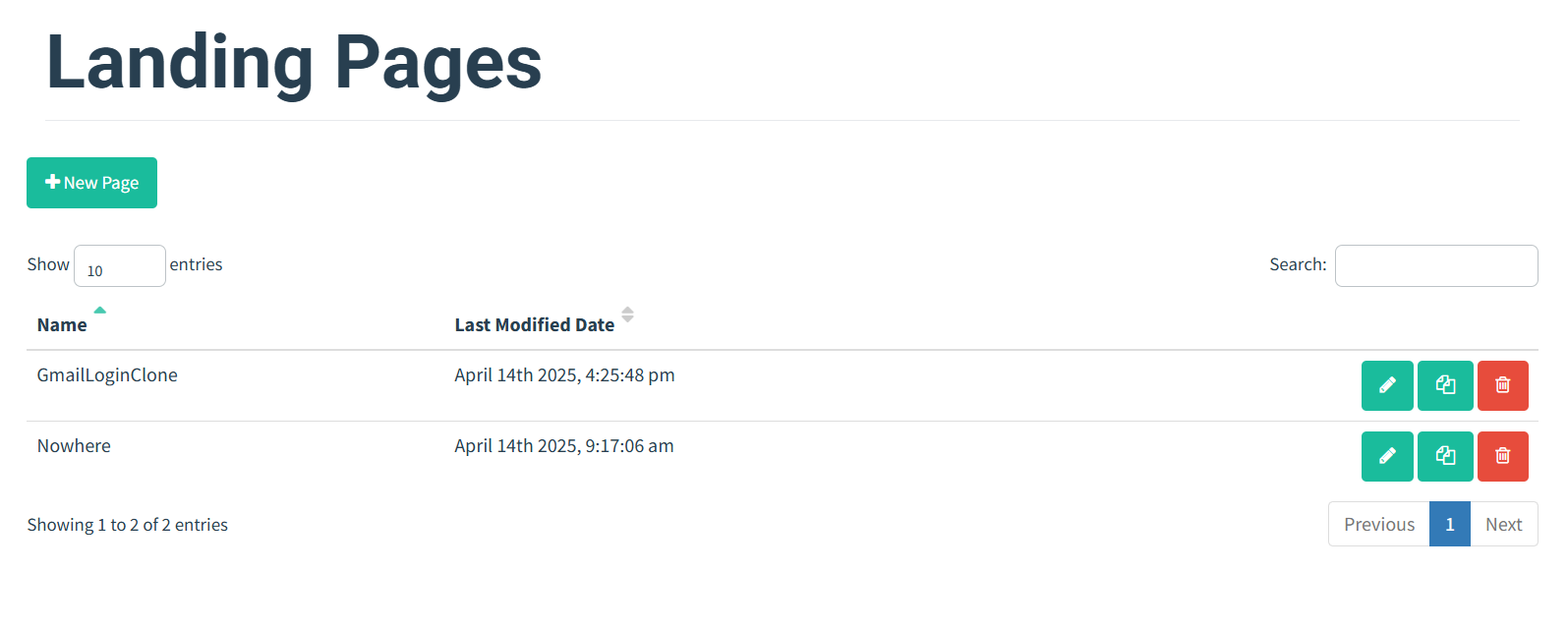
#### Recipients:

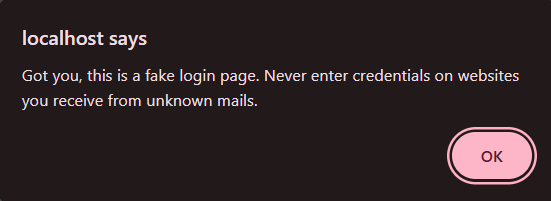
10 emails were sent to friends in a controlled environment for testing purposes.



#### Landing Page:

* The provided link in the email redirected to a Gmail login clone where users were prompted to enter their email and password.
* Upon submission, the credentials were captured by Gophish.
* Users who entered their credentials were then shown an alert message, warning them about the fake login page and advising them never to enter credentials on websites received through unknown emails.





#### Results:

##### Phishing Success Rate:

##### **7/10** recipients engaged with the phishing campaign, either by clicking the link or entering their credentials.

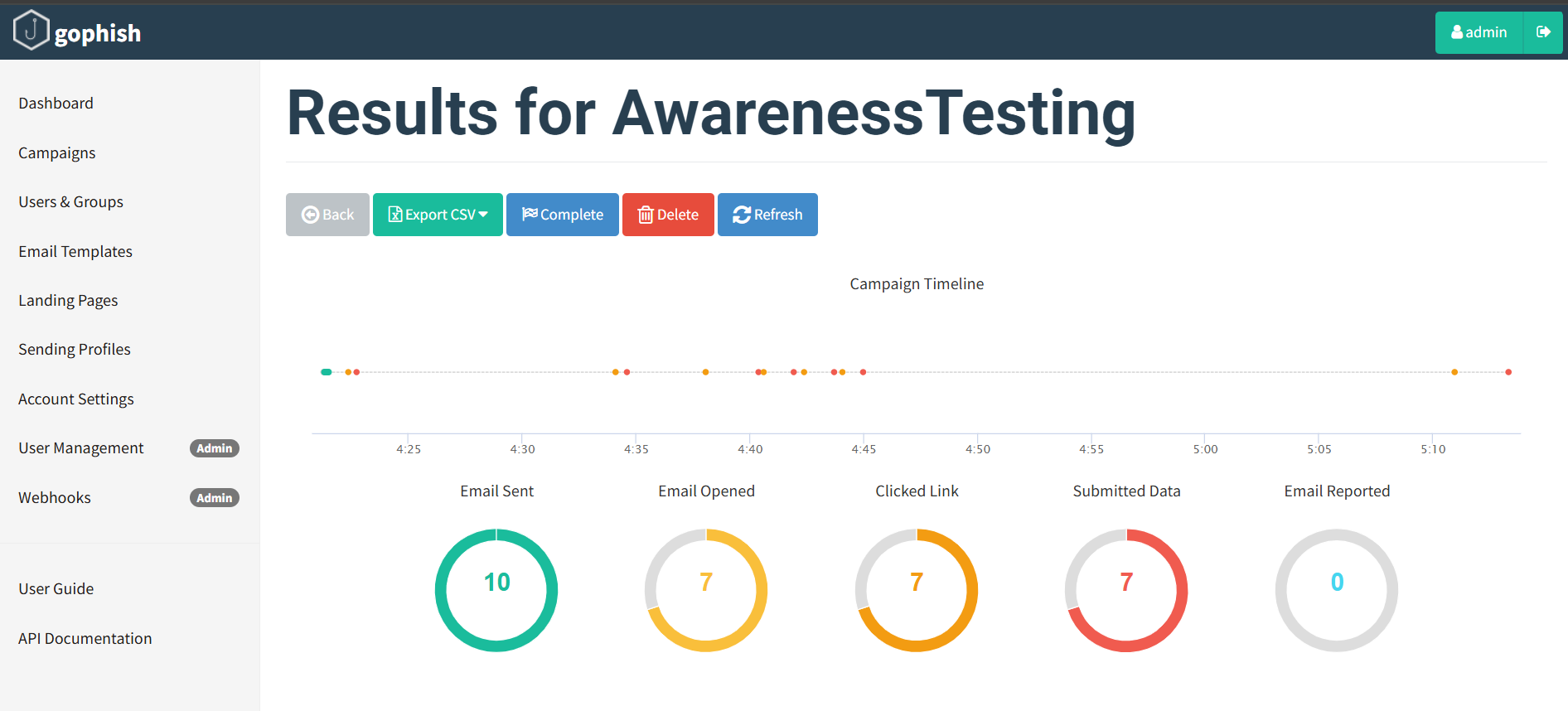
* **70% success rate** in terms of engagement, indicating a relatively high susceptibility to this phishing tactic.

##### Credential Harvesting:

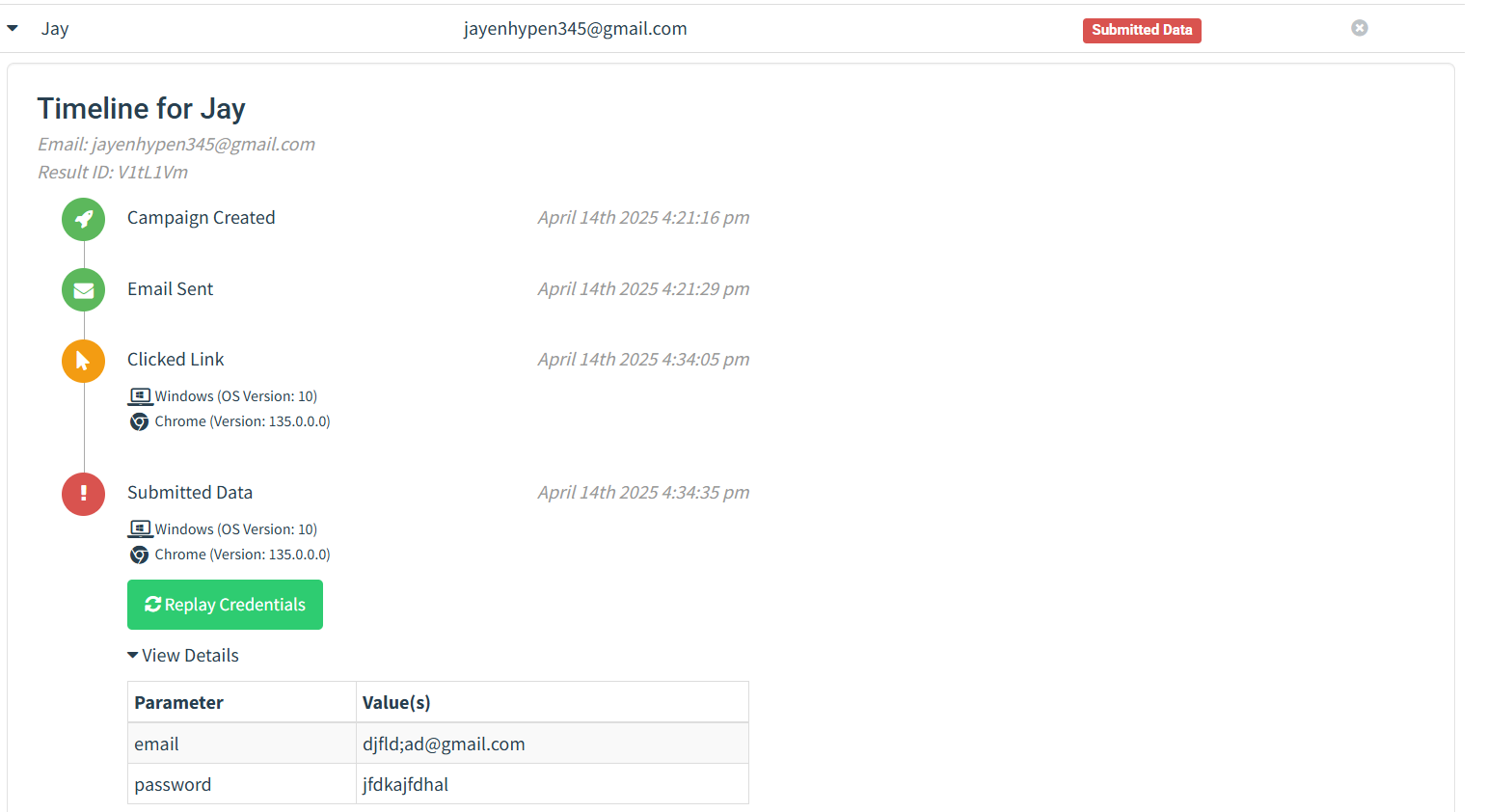
* Credentials from 7 recipients were successfully captured, showing that the phishing technique was effective in this controlled environment.

##### User Awareness:

* After entering their credentials, users were shown an alert stating: *"Got you, this is a fake login page. Never enter credentials on websites you receive from unknown mails."*
* This message served as an immediate feedback mechanism to inform users about their mistake.



Example of captured details:



|  |  |  |
| --- | --- | --- |
| Metric | Count | Description |
| Emails Sent | 10 | Total Emails delivered to users |
| Emails Opened | 7 | Number of users who opened the email. |
| Link Clicked | 7 | Users who clicked the phishing link. |
| Submitted Data | 7 | Users who entered credentials or other data. |
| Emails Reported | 0 | |  | | --- | |  |  |  | | --- | | Users who reported the email as suspicious. | |

#### ****Analysis of Results:****

* Out of the 10 emails sent, 7 recipients responded to the phishing emails. This indicates a high level of interaction, suggesting that the phishing tactics used were effective at luring recipients into engaging with the content.
* It also highlights that many employees or individuals may be susceptible to social engineering attacks, especially phishing attempts that create a sense of urgency or appeal to their concerns (e.g., checking for suspicious activity in their account).
* This test also demonstrated that people may not always be cautious when receiving unsolicited emails that request sensitive information, especially when the email appears to come from a seemingly legitimate source.

#### Recommendations for Security Awareness Training:

Based on the results of this phishing campaign, the following actions are recommended to improve overall employee awareness:

##### Enhanced Phishing Detection Training:

* Educate employees on how to identify common phishing signs, including suspicious email addresses, unsolicited links, and requests for sensitive information.
* Provide real-world examples of phishing emails to aid recognition.

##### Simulated Phishing Drills:

* Conduct regular simulated phishing attacks as part of ongoing security training to test employees' ability to spot phishing emails. These exercises will also help employees practice identifying phishing attempts in a safe environment.
* Measure response rates and tailor training programs based on the results.

##### Improved Email Security Awareness:

* Encourage employees to verify the legitimacy of unexpected or suspicious emails by reaching out to the sender through official communication channels.
* Ensure that employees understand the importance of email security measures like SPF, DKIM, and DMARC to prevent spoofed emails from being delivered to inboxes.
* Promote the use of email security tools, such as email filtering, and educate employees on how to report suspicious emails.

##### Actionable Security Measures:

* Enforce multi-factor authentication (MFA) for all accounts to reduce the impact of a successful phishing attack. MFA adds an additional layer of security, making it more difficult for attackers to gain unauthorized access.
* Create a clear process for reporting suspected phishing attempts within the organization.

#### Conclusion:

This phishing campaign successfully simulated a common attack vector and revealed valuable insights into recipient susceptibility. The high response rate underscores a clear need for improved awareness and training, particularly in recognizing the signs of phishing emails. Moving forward, implementing a structured security awareness program and conducting regular phishing simulations will be essential in reducing the risk of such attacks and strengthening the organization's overall security posture.

**Report Prepared By:** M.Sahiti

**Contact:** sahitim137@gmail.com