Simulated Phishing Campaign Report

Report Prepared By: *Linto Baby*

Executive Summary

This report details a small-scale, end-to-end simulated phishing attack executed using the **GoPhish** framework. The campaign, which featured an urgent Google 2FA email leading to a cloned Facebook login page, achieved a **100% compromise rate** on the single test account. The primary goal was successfully met: to demonstrate that a basic phishing setup can quickly and effectively harvest credentials. The findings confirm that users are highly susceptible to urgent email lures and deceptive landing pages, underscoring the necessity of continuous security awareness training.

---

1. Introduction: Setting the Scope

The aim of this exercise was to establish a technical proof-of-concept for a **credential harvesting attack**. We utilized **GoPhish** on a Kali Linux environment to simulate a real-world social engineering attempt. While this test was confined to a single account, the successful outcome proves the entire attack chain—from email delivery to data theft—is fully functional.

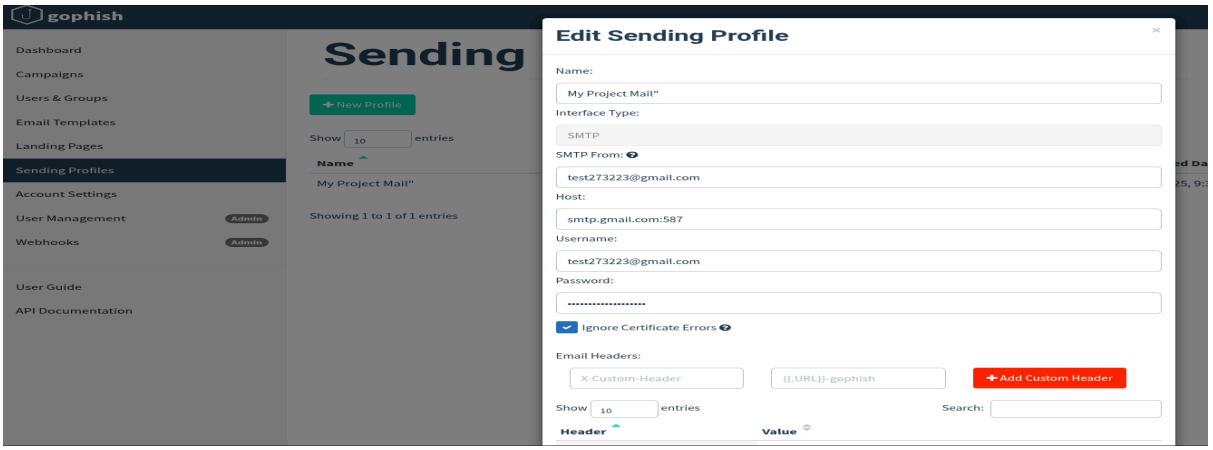
---

2. Campaign Methodology: The Attack Walkthrough

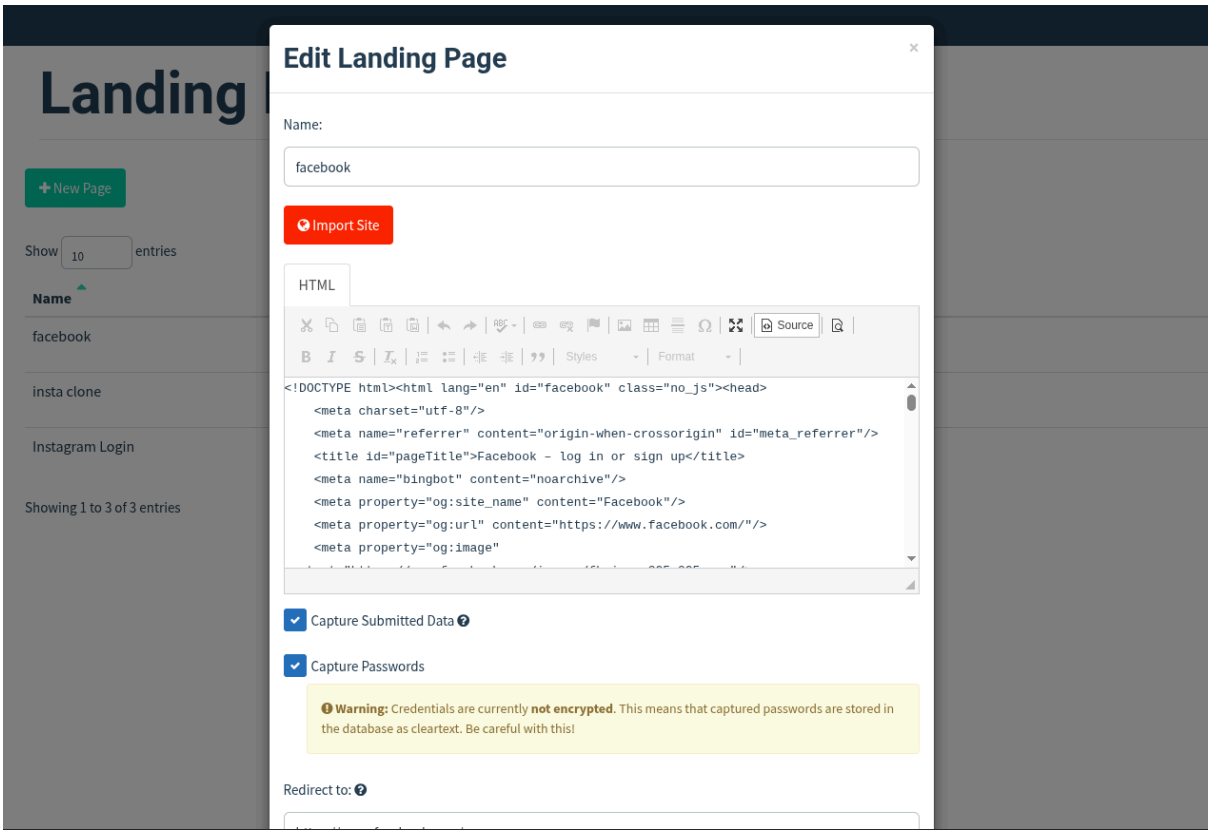
The phishing simulation was designed and executed in the following straightforward stages:

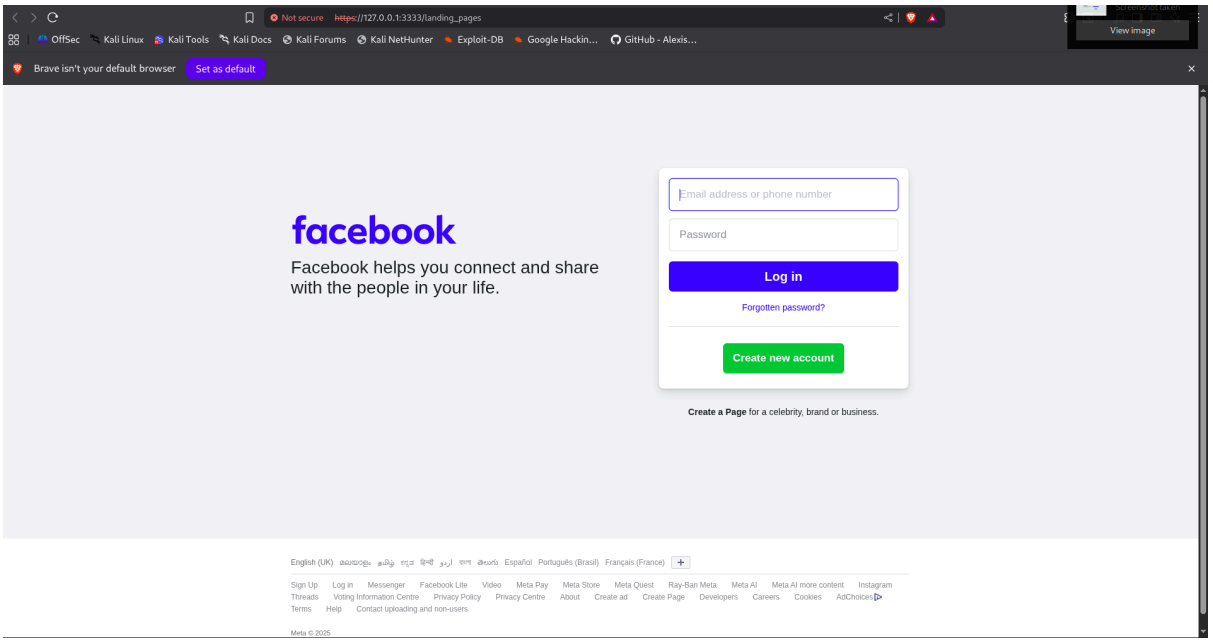
2.1. GoPhish Environment Setup

1. **Sending Profile:** We first set up a dedicated **Sending Profile** (My Project Mail) within GoPhish, routing all outbound emails through a newly created Gmail account using **smtp.gmail.com:587**. This ensured successful delivery to the target.

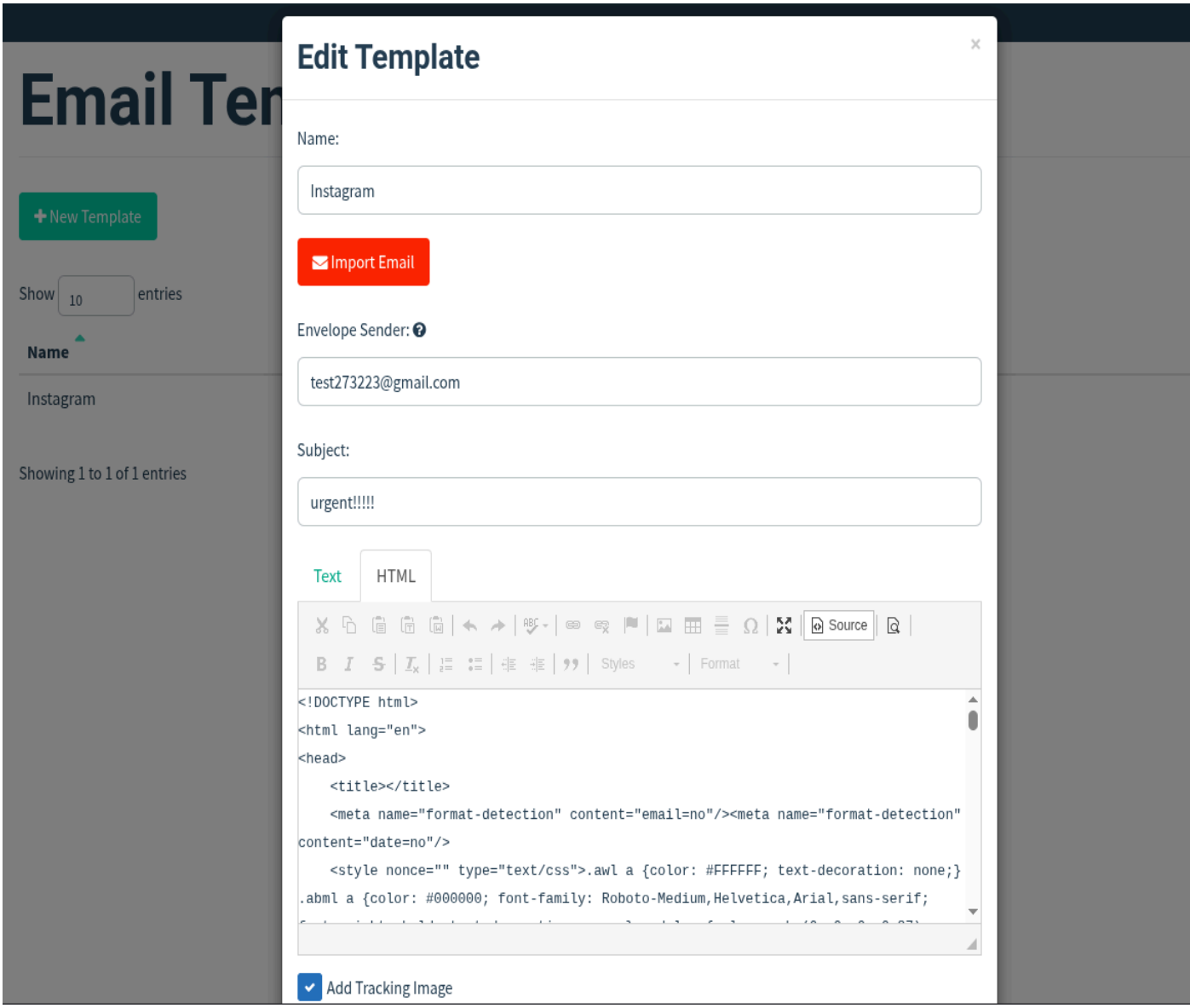


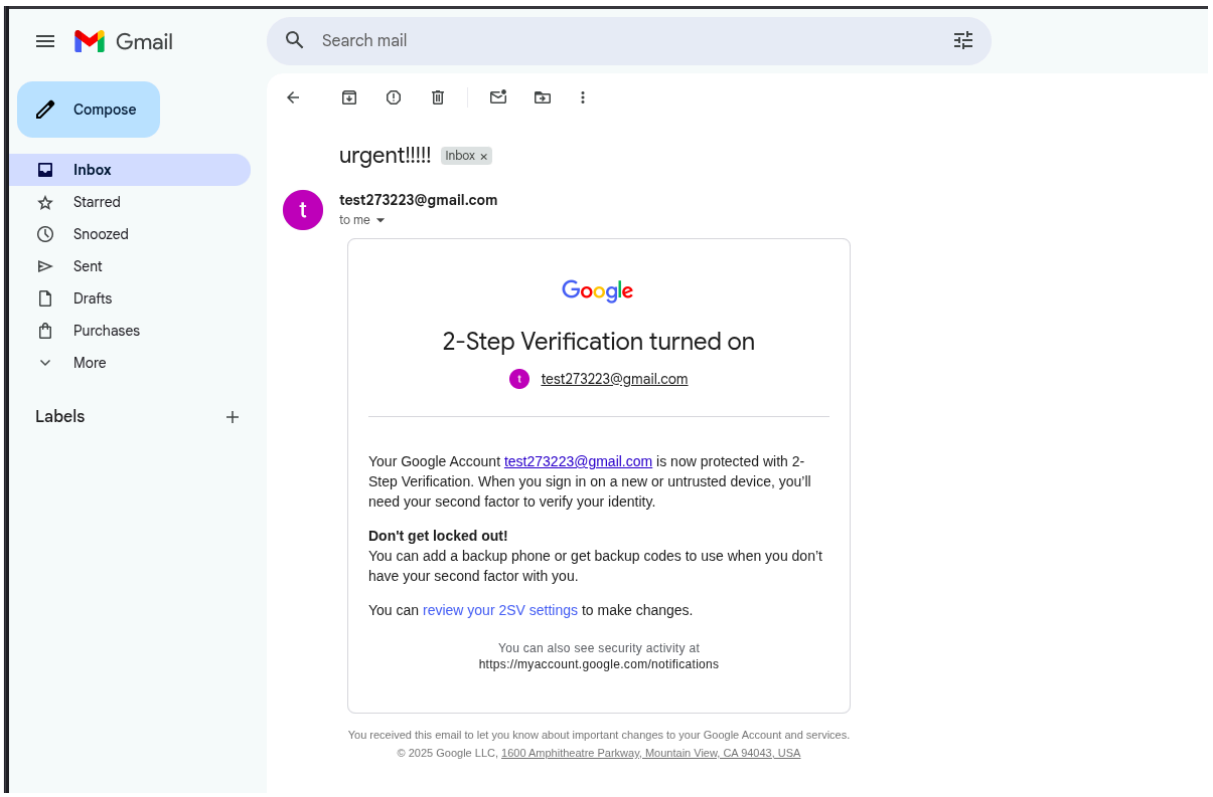
2. **Landing Page Lure:** The core of the attack was a deceptive login page. We used GoPhish's cloning feature to create an exact replica of the official **Facebook login page**. Crucially, the page was configured to **capture all submitted data** (the fake username and password) before automatically **redirecting** the user to the legitimate Facebook site, making the compromise seamless and hard to spot.





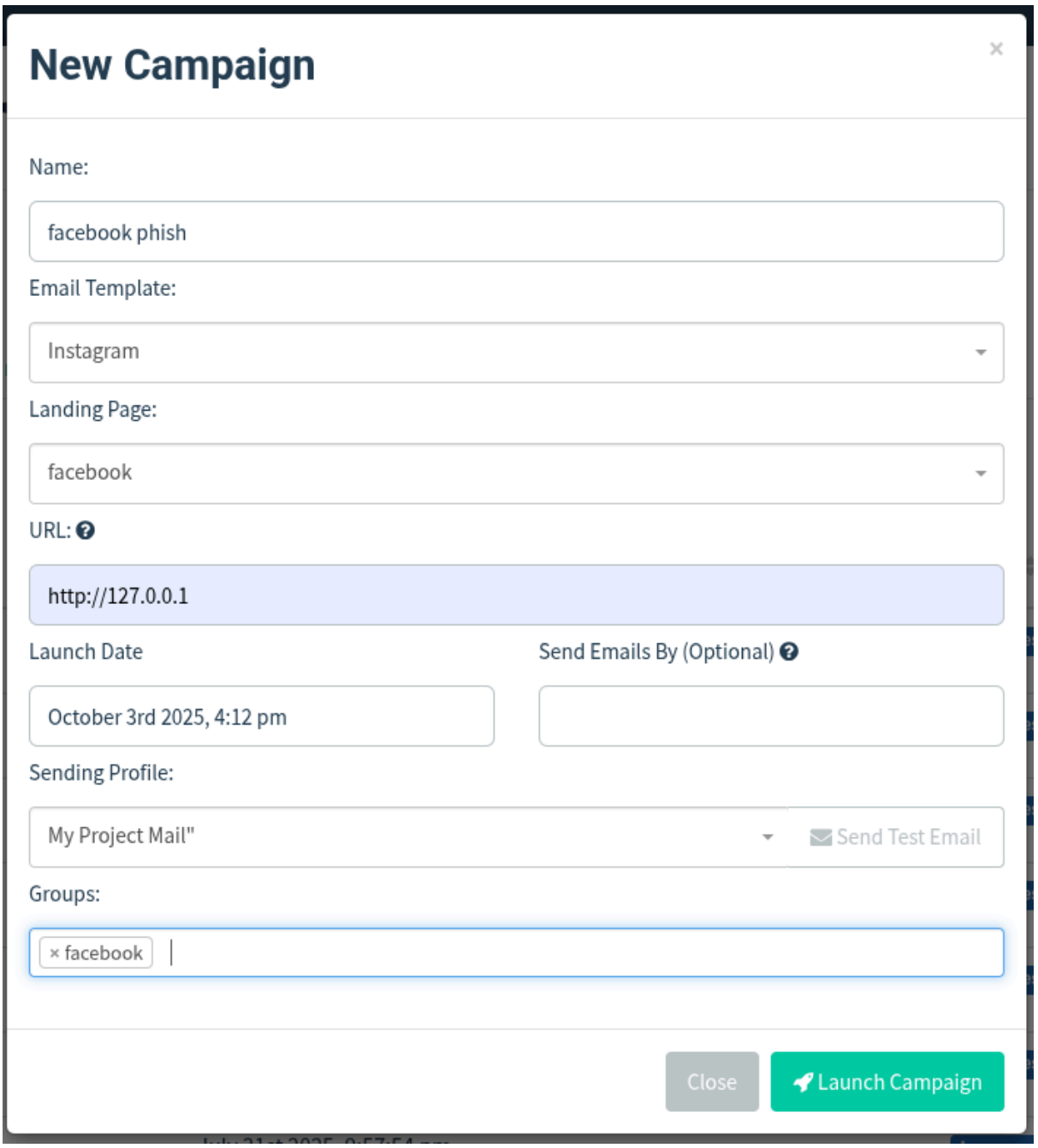
3. **Email Template:** To drive clicks, we designed a high-urgency email. The body was a spoofed **Google 2-Step Verification alert** (subject: urgent!!!!!) that told the user to take immediate action. (*Note: This lure was intentionally mismatched with the Facebook landing page for this initial technical test, but was effective at getting the click.*).

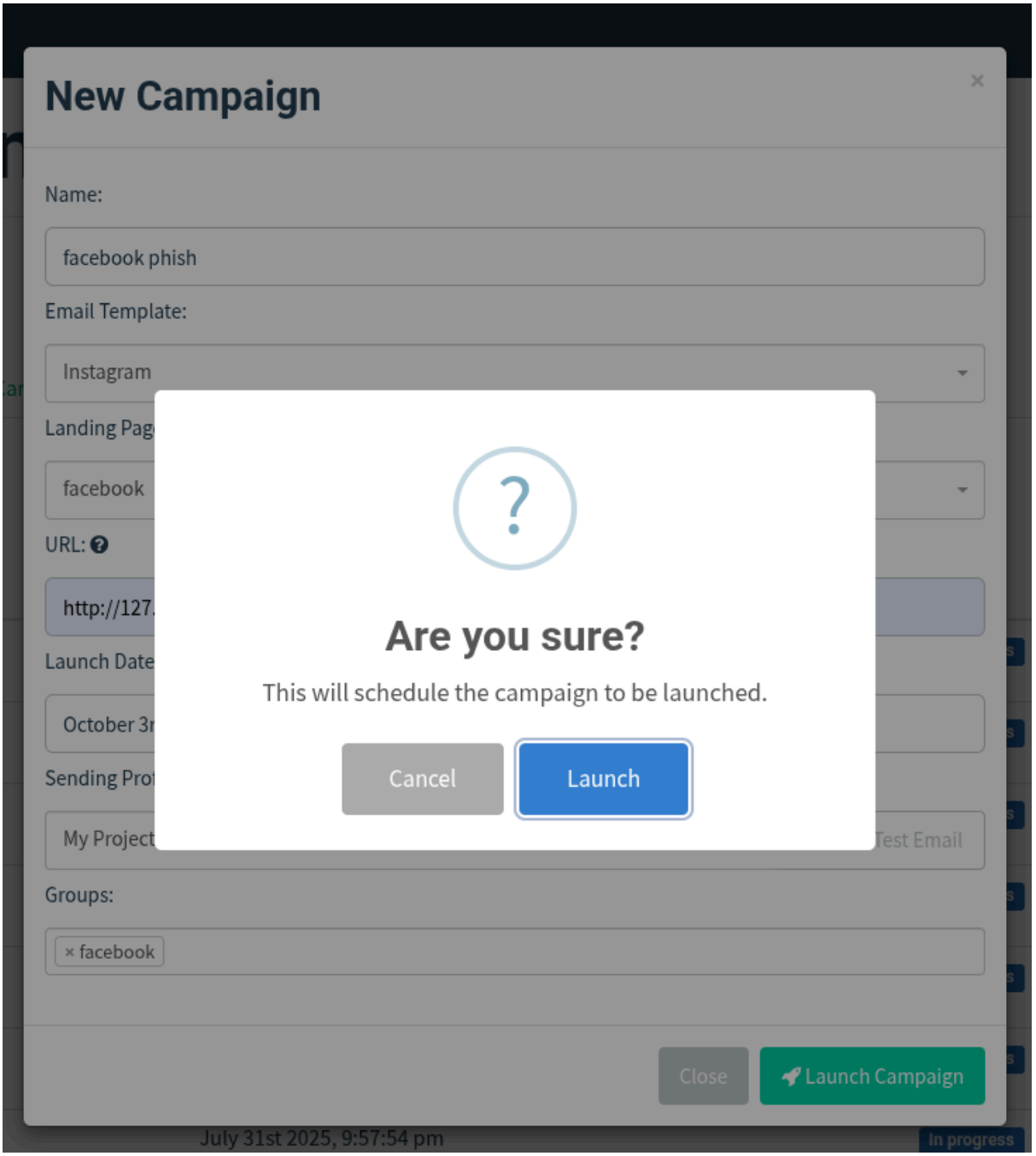


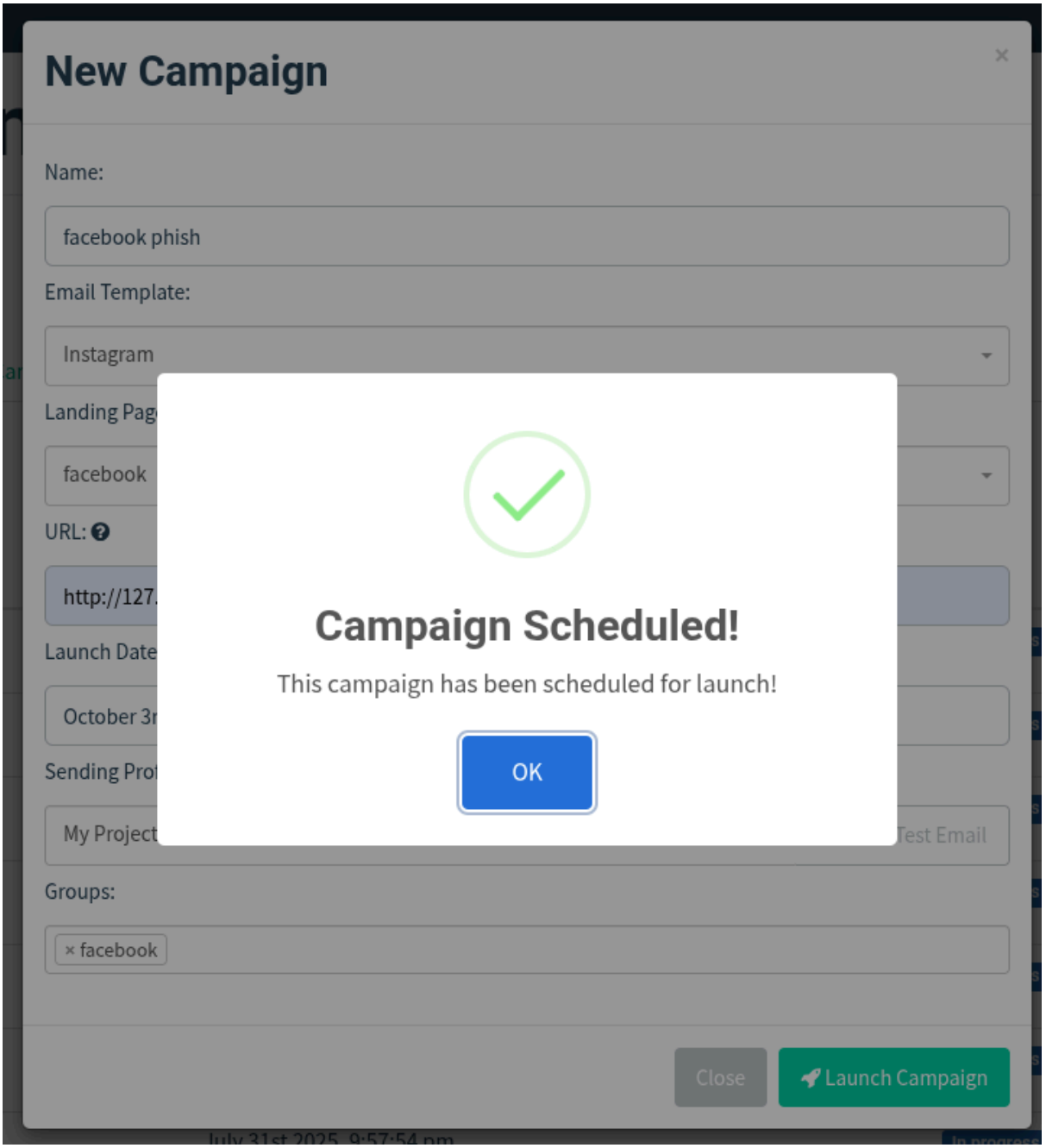


2.2. Campaign Execution

The campaign, named **facebook phish**, was configured to use all the components above and was launched on **October 3rd, 2025**. The target was the single test account, **test273223@gmail.com**. We used the local http://127.0.0.1 as the deceptive link URL for this initial test.


New Campaign
Name:
facebook phish
Email Template:
Instagram
Landing Page:
facebook
URL:
http://127.0.0.1
Launch Date
October 3rd 2025, 4:12 pm
Send Emails By (Optional)
Sending Profile:
My Project Mail"
Send Test Email
Groups:
facebook
Close
Launch Campaign


New Campaign
Name:
facebook phish
Email Template:
Instagram
Landing Pag
facebook
URL:
http://127.
Launch Date
October 3r
Sending Pro
My Project
Test Email
Groups:
× facebook
Are you sure?
This will schedule the campaign to be launched.
Cancel
Launch
Close
Launch Campaign
July 31st 2025, 9:57:54 pm
In progress



---

3. Results and Analysis: The Compromise

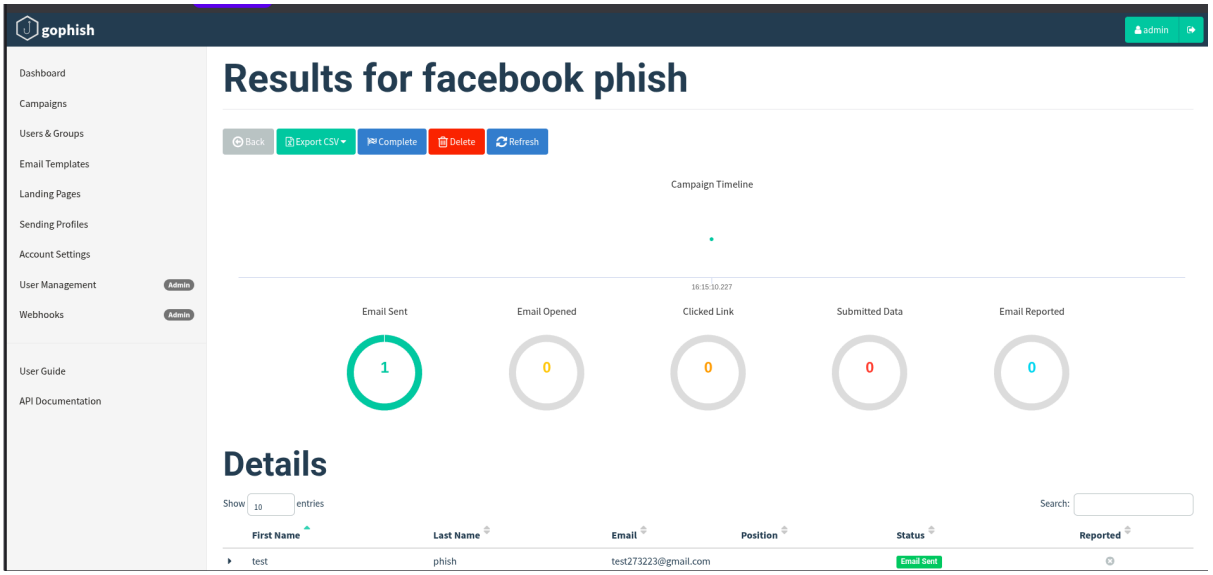
The attack chain was 100% successful, validating the technical integrity of the setup.

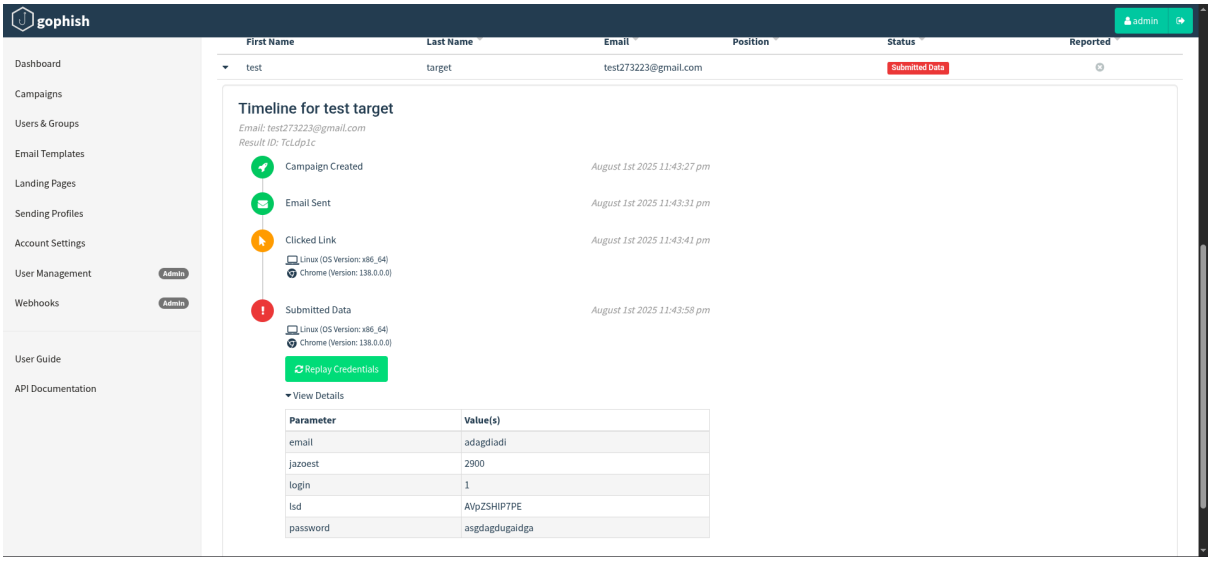
Metric	Outcome
Email Delivered & Opened	1 out of 1 (100%)

Link Clicked	1 out of 1 (100%)
Credentials Submitted	1 out of 1 (100%)

The GoPhish metrics immediately confirmed the successful compromise: the test user opened the email, clicked the urgent link, and then—most critically—entered login details into the cloned Facebook form.

The **cred.png** screenshot confirms that the platform successfully harvested the submitted password and associated data. This result proves that if we used a more realistic, large-scale target list and a less-obvious URL, this method would be highly effective for a wide-scale credential harvesting attack.





---

4. Conclusion and Next Steps

This successful simulation confirms that the current environment is vulnerable to credential harvesting via phishing campaigns. The next steps should be directed at increasing the realism of the simulation for large-scale employee testing and reinforcing user education.

Recommendations:

1. **Improve Realism:** Future campaigns must drop the local IP (`127.0.0.1`) and use an externally hosted, deceptive domain name to better mimic a real attack.
2. **Thematic Alignment:** Ensure the email lure and the landing page are perfectly aligned (e.g., a Microsoft 365 security alert leading to a cloned M365 login) to maximize the psychological impact.
3. **Expand Scope:** The next simulation needs to target a statistically significant group of employees (e.g., an entire department) to establish a true organizational susceptibility metric.
4. **Immediate Training:** Based on the ease of compromise demonstrated here, **immediate and mandatory re-training** should be scheduled for employees on the fundamentals of spotting deceptive URLs and recognizing social engineering tactics.