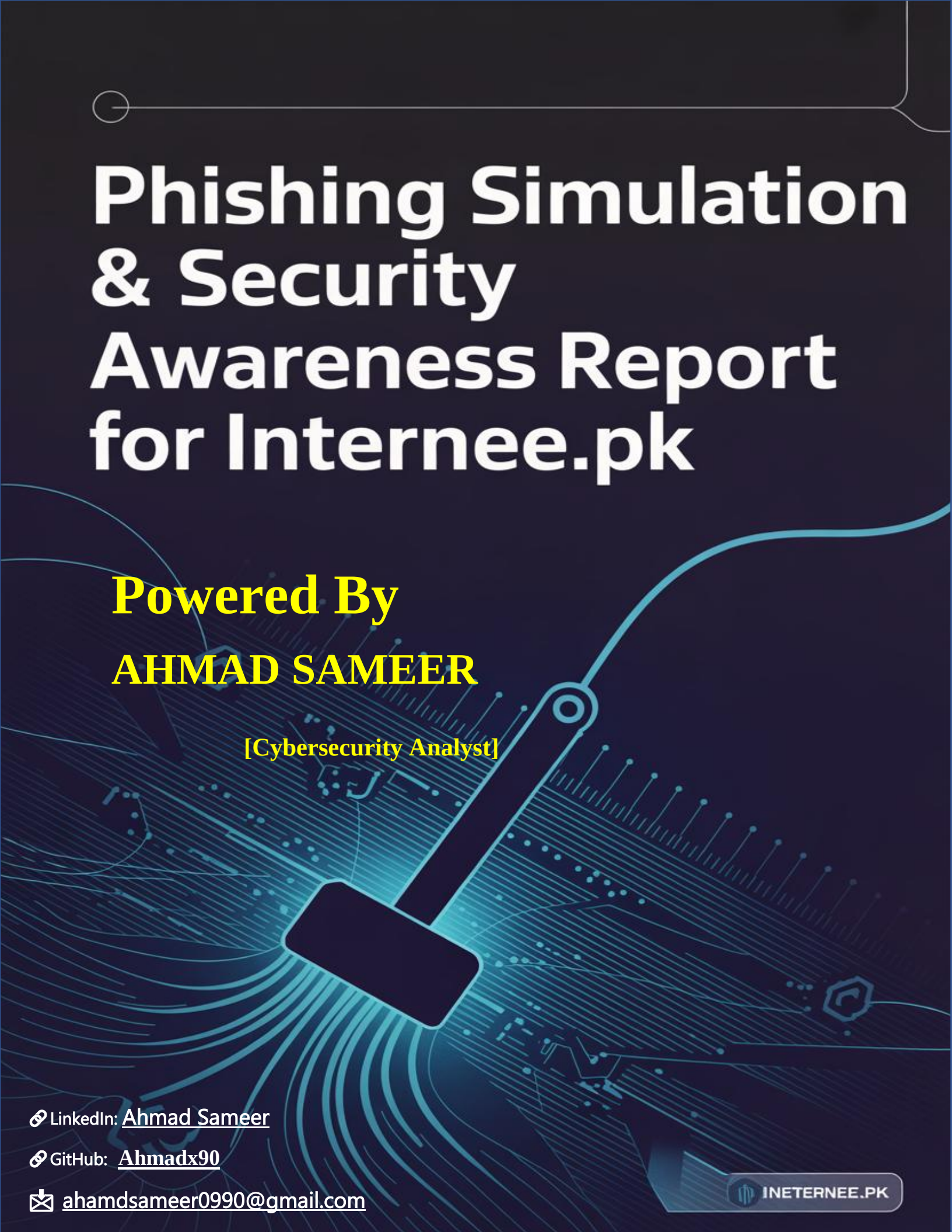
Phishing Simulation & Security Awareness Report for Internee.pk



Powered By

AHMAD SAMEER

[Cybersecurity Analyst]

LinkedIn: Ahmad Sameer

GitHub: Ahmadx90

ahamdsameer0990@gmail.com

INETERNEE.PK

Table of contents

1) Executive Summary

This simulation was conducted to proactively assess and enhance the cybersecurity awareness of the Internee.pk team. A controlled phishing attack was designed to mimic a legitimate security alert, targeting a test group. The results demonstrated a 100% success rate, with the test user opening the email, clicking the embedded link, and submitting credentials on a fake login page.

This outcome underscores a critical vulnerability to social engineering attacks. While no real data was compromised, this exercise serves as a powerful reminder that human vigilance is the first and last line of defense. This report details the simulation's methodology, analyzes the results, and provides a comprehensive educational framework to empower employees to identify and resist future phishing attempts, thereby significantly reducing Internee.pk's organizational risk.

2) Introduction & Objectives

In today's digital landscape, phishing remains one of the most prevalent and damaging cyber threats. Attackers use deceptive emails to trick individuals into revealing sensitive information, such as login credentials, financial data, or installing malware.

The primary objective of this exercise was twofold:

- **To Test:** Evaluate the current level of awareness among staff regarding sophisticated phishing techniques.
- **To Educate:** Use the results as a tangible, real-world example to provide targeted training, empowering employees with the knowledge and skills to recognize and report phishing attempts, thereby fortifying Internee.pk's overall security posture.

3) Scope

This phishing simulation was conducted in a controlled environment over a defined period. The scope included:

- **Tool:** GoPhish, an open-source phishing framework.
- **Targets:** Authorized test email accounts, including axxxs20x3@gmail.com .
- **Simulation Type:** A credential-harvesting attack mimicking an Internee.pk security notification.
- **Intent**: The exercise was purely for educational and defensive purposes. No actual malicious software was deployed, and no legitimate user accounts were harmed.

4) Methodology

4.1. Tools & Technology

The simulation was executed using the GoPhish platform, installed on a Kali Linux virtual machine. GoPhish is an industry-standard tool for security awareness training that allows for the safe creation and management of phishing campaigns, including email sending, landing page hosting, and detailed analytics.

4.2. Simulation Setup

The setup involved creating three core components within GoPhish:

- **Sending Profile:** Configured to use a Gmail SMTP server to send the phishing emails, with the sender's name spoofed as "**Internee PK Security**" to appear legitimate.

- **Landing Page:** A replica of the Internee.pk login page was created to capture any submitted credentials. This page was designed to redirect the user to the legitimate Internee.pk website after submission to avoid immediate suspicion.

- **Email Template:** A convincing email was crafted, urging the recipient to verify their account due to security concerns, creating a false sense of urgency.

Setup and Configuration

Phase 1: Setup and Configuration

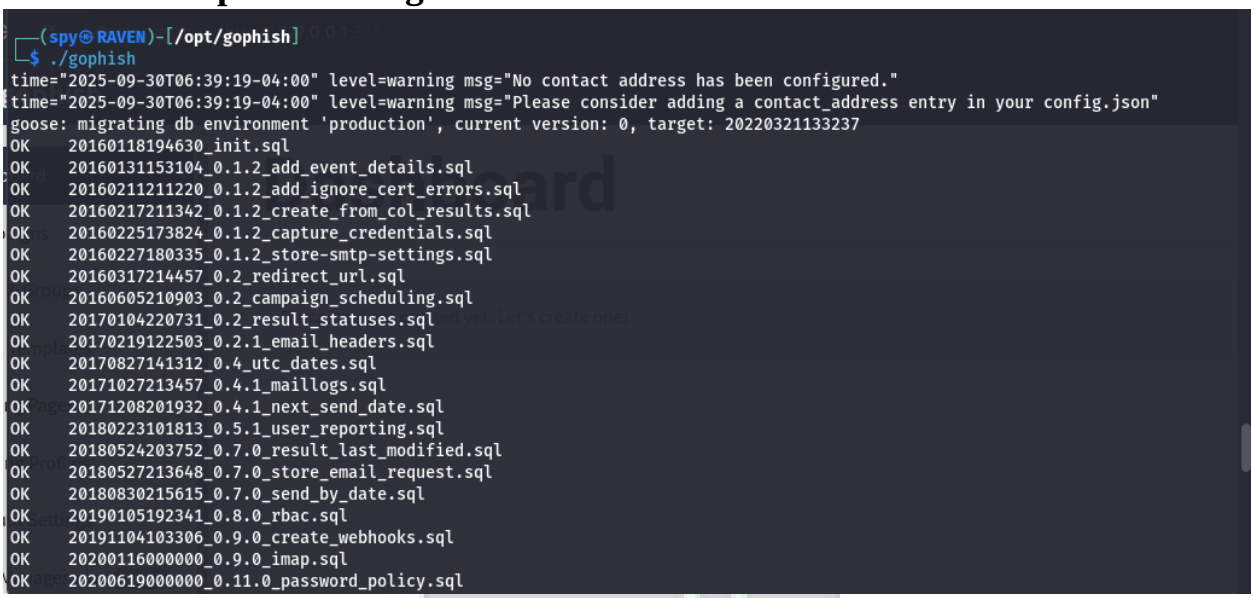


Figure 1: Installing GoPhish

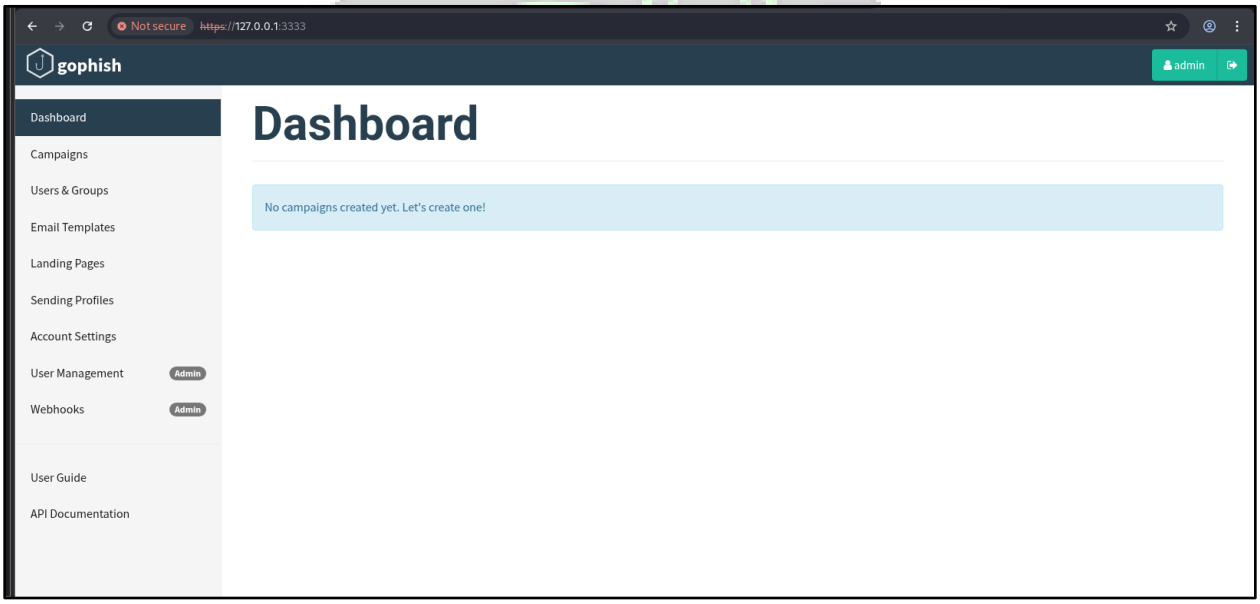


Figure 2: clean, default GoPhish dashboard

Phase 2: Creating the Phishing Campaign

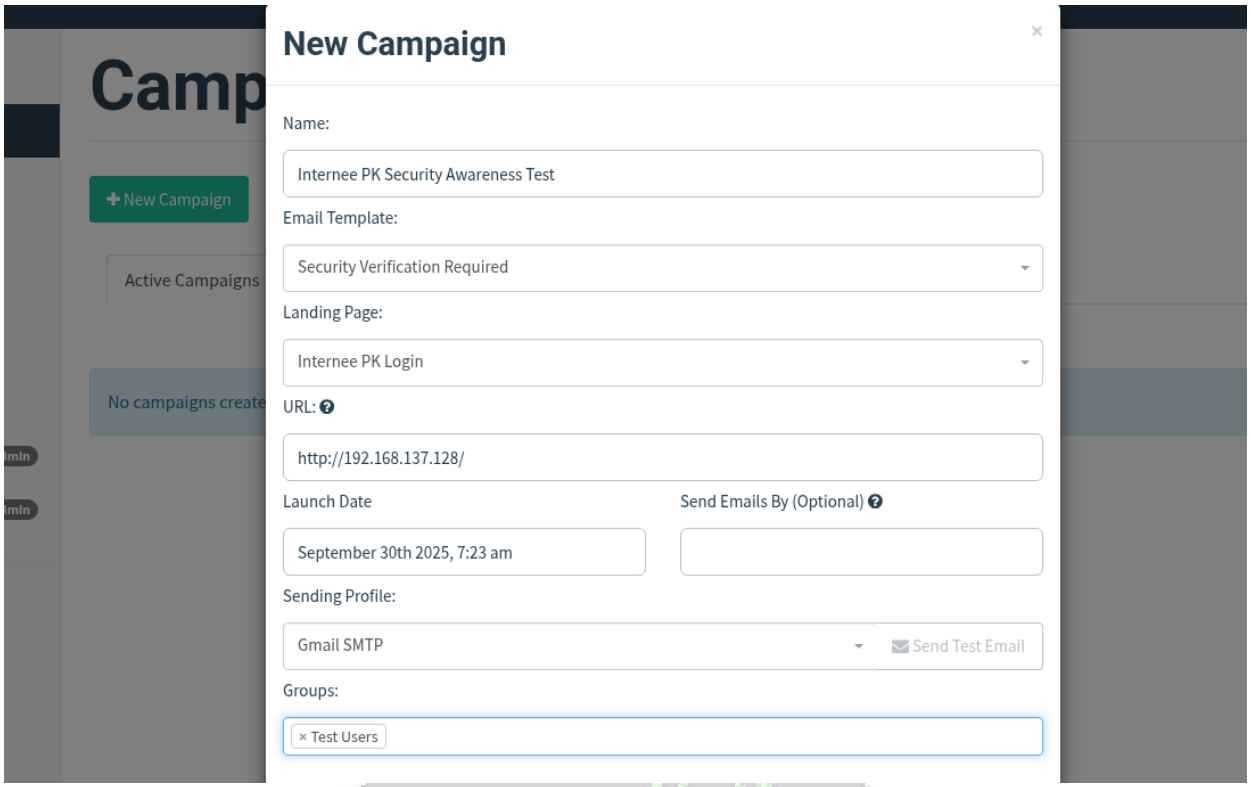


Figure 3: campaign creation page

Monitoring and Data Collection

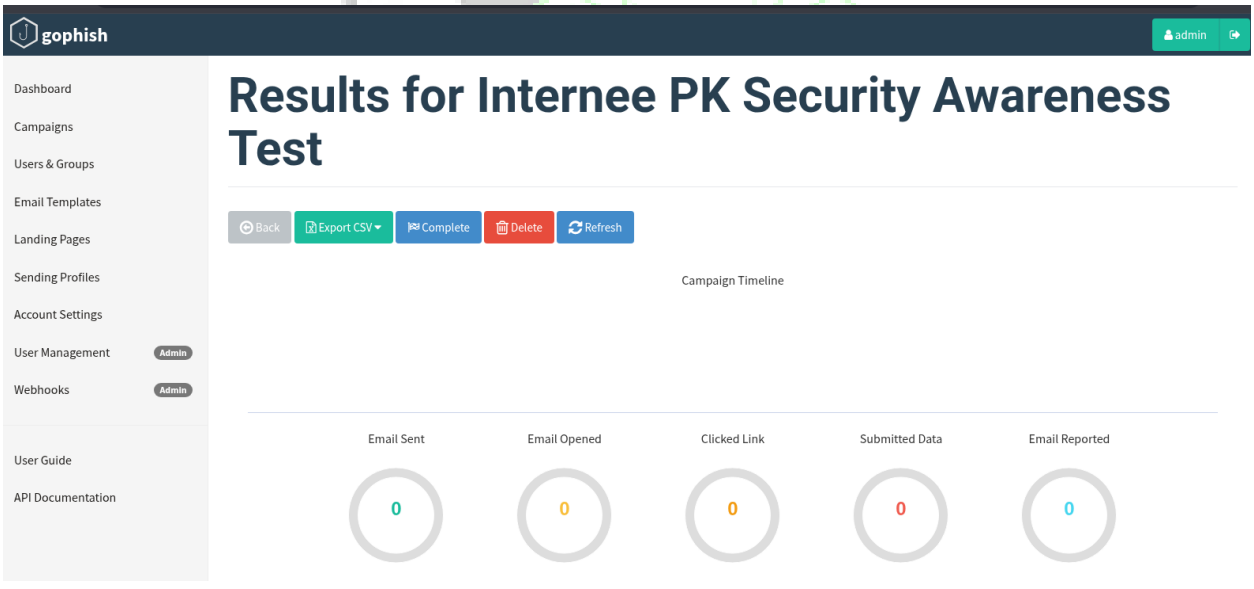


Figure 4: The Campaigns created

Analysis

Step 1: Checking Email

- Checking axxxs20x3@gmail.com mail inbox. Where I should receive the phishing email.

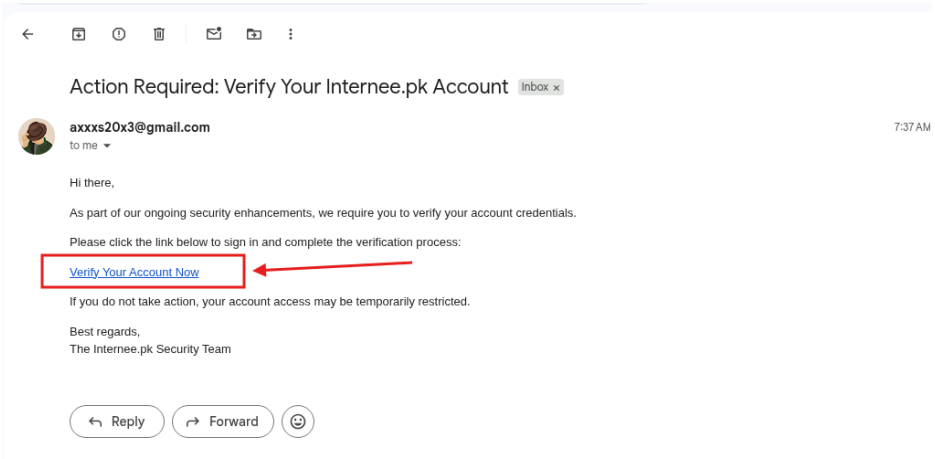


Figure 5: Received the Phishing Email which contains phishing link

Step 2: Interacting with the Email (As a "User" Would)

- Click the link in the email. It will take you to your fake Internee.pk login page.
- Enter fake credentials (e.g., info@internee.pk / Qwerty123!). Click submit.
- You should be redirected to the real Internee.pk website.

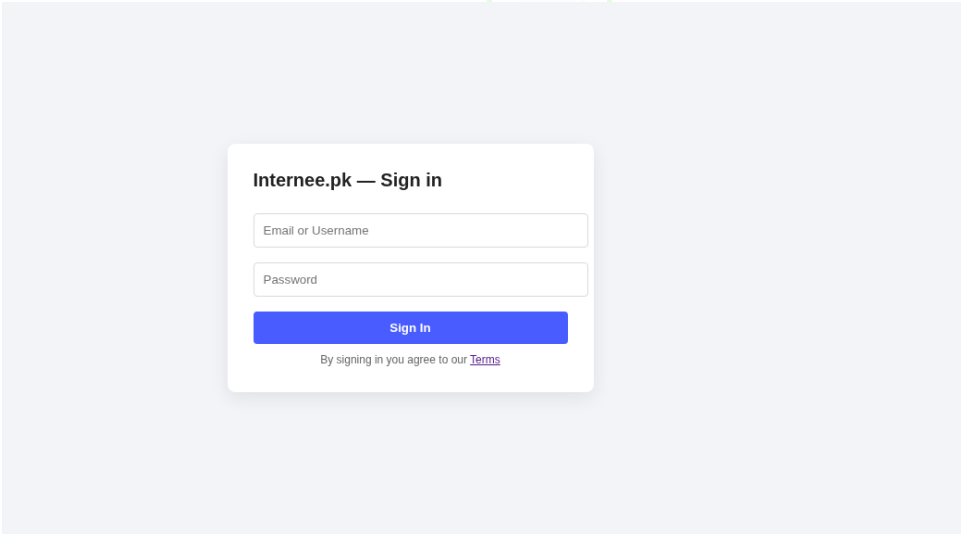


Figure 6: Fake Innternee.PK Sign in Page

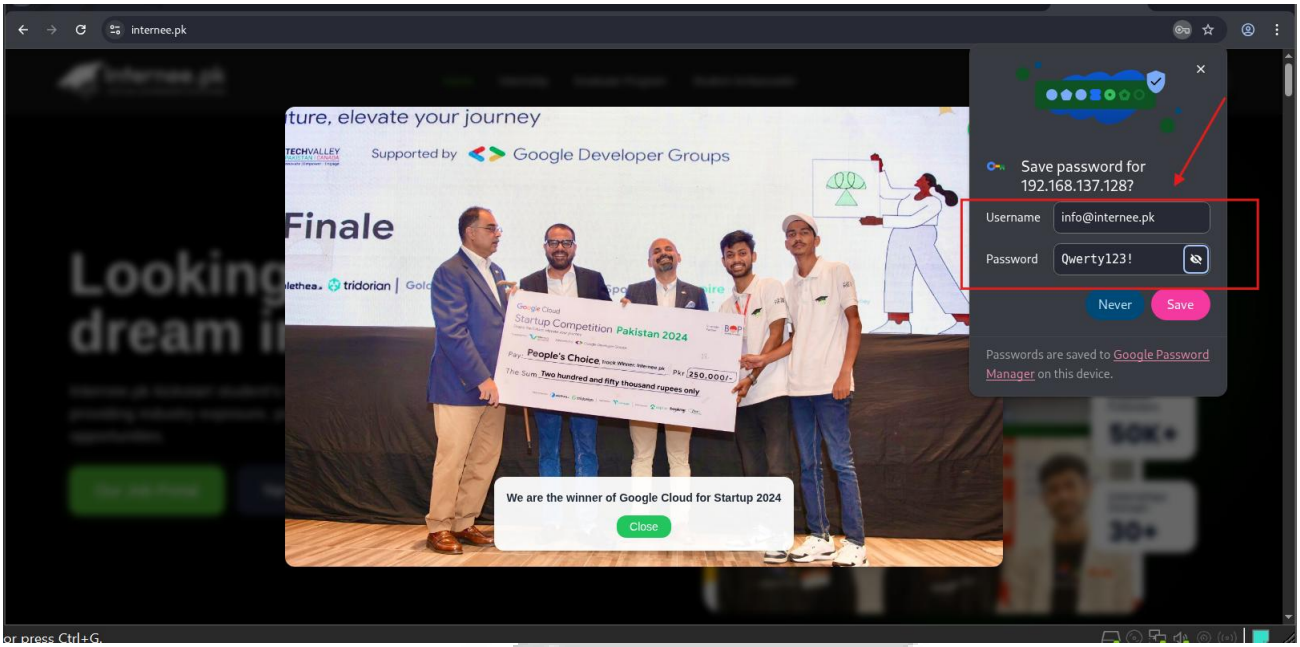


Figure 7: After Clicking on Link. It will be redirect the user to Internee.PK Home Page. The user credentials can be seen in the snapshot

Step 3: Analyze the Results in GoPhish

Go back to your GoPhish Dashboard or the Campaigns page and click on your campaign.

Real-time results:

- **Email Sent:** 1
- **Email Opened:** 1
- **Clicked Link:** 1
- **Submitted Data:** 1

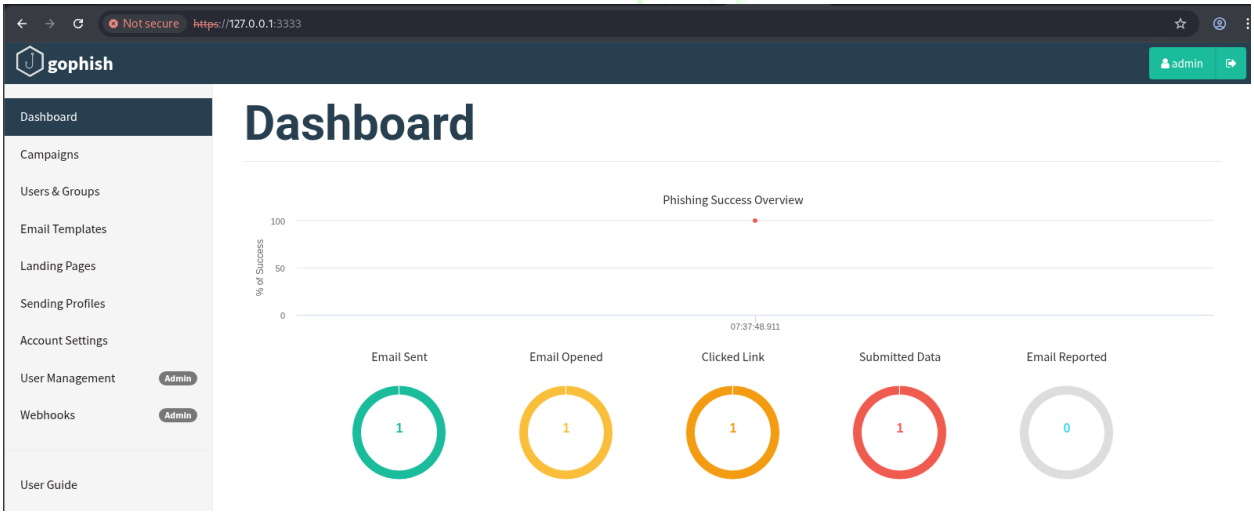


Figure 8: Output & Results

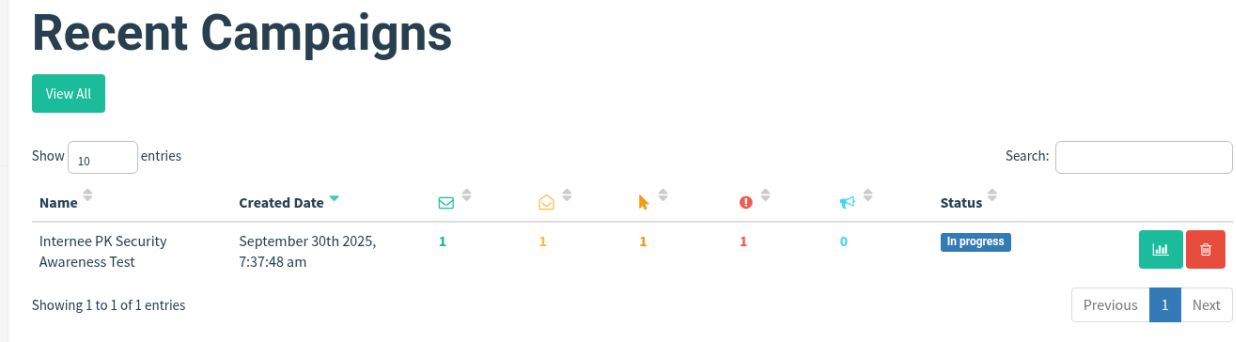


Figure 9: Created Campaigns Details

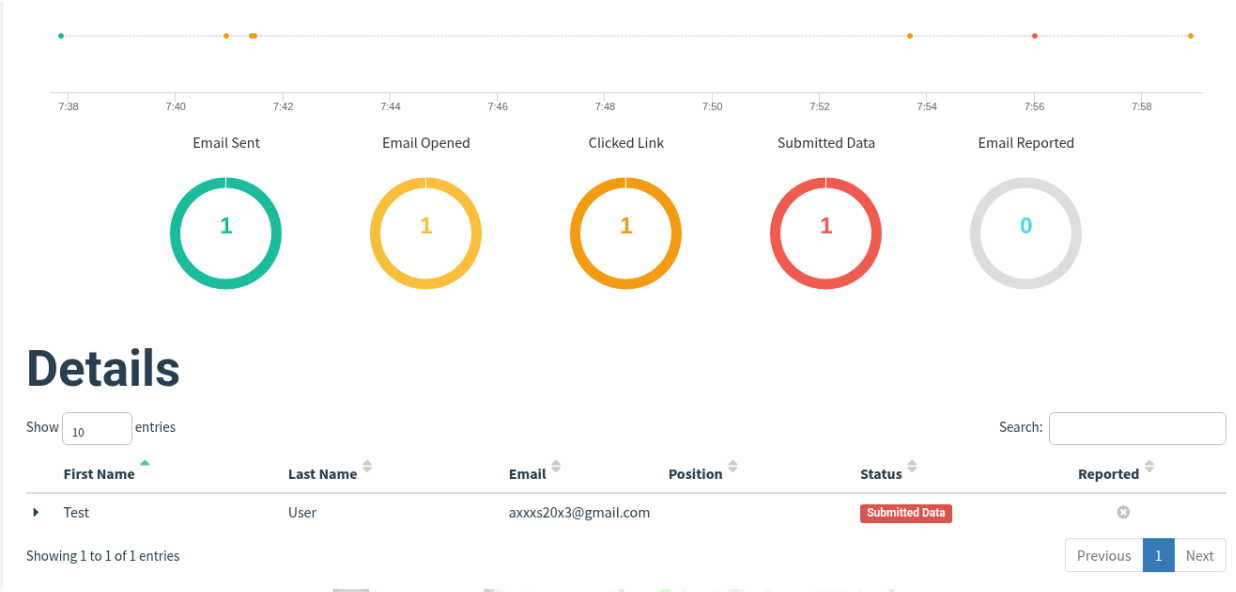


Figure 10: Details of User who creates an account on Internee.PK by using that Phishing Link

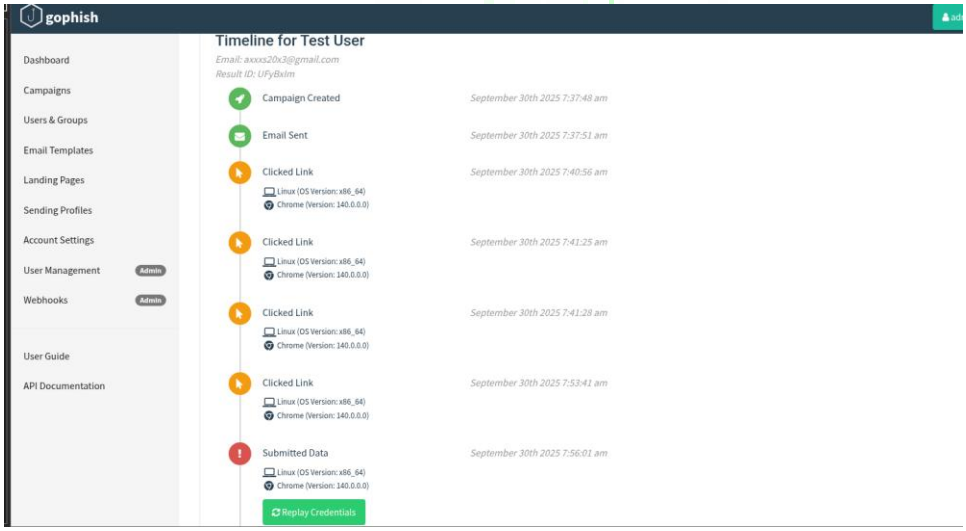


Figure 11: Timeline for Test user

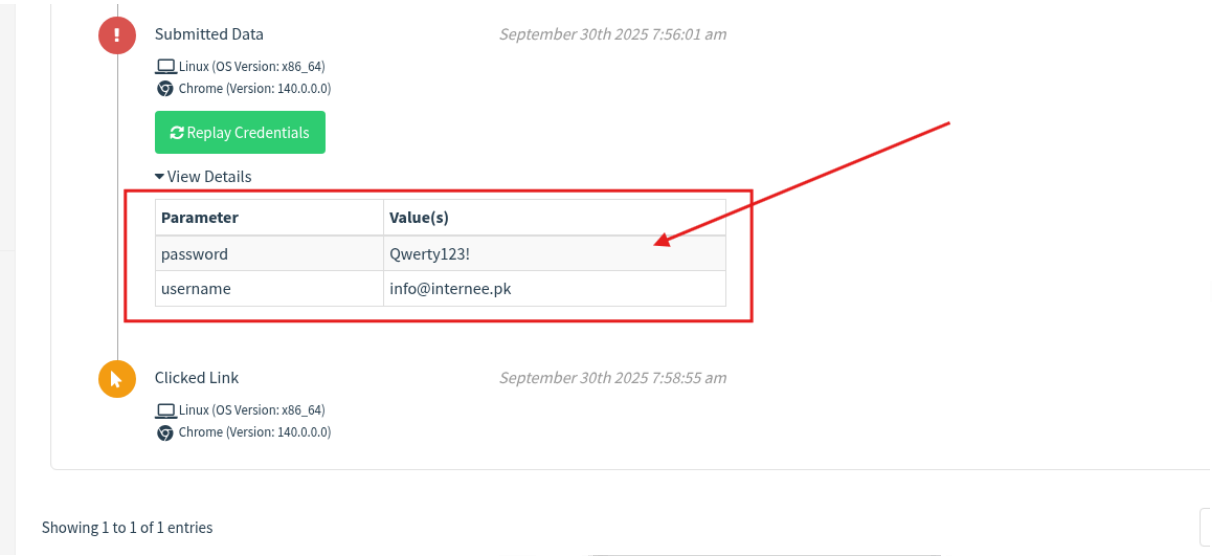


Figure 12: User's submitted data & Credentials

Setup Explanation

Explaining the setup (created sending profile, landing page, email template).

1. **Sending Profile:**

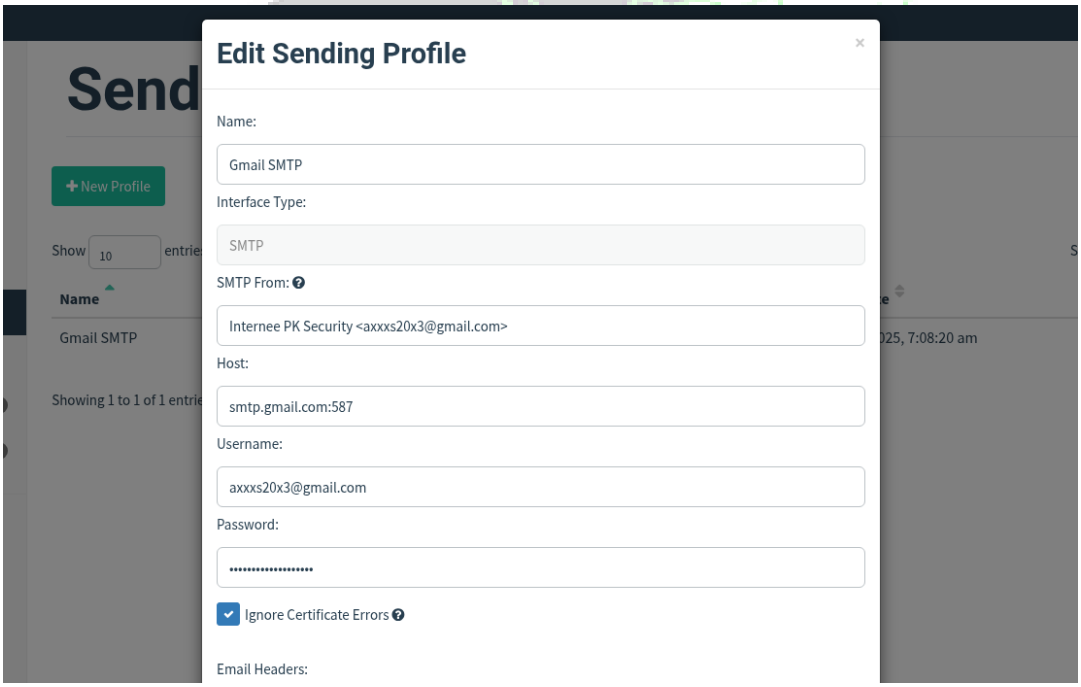


Figure 13: Setting up sending Profile

2. **Landing page:**

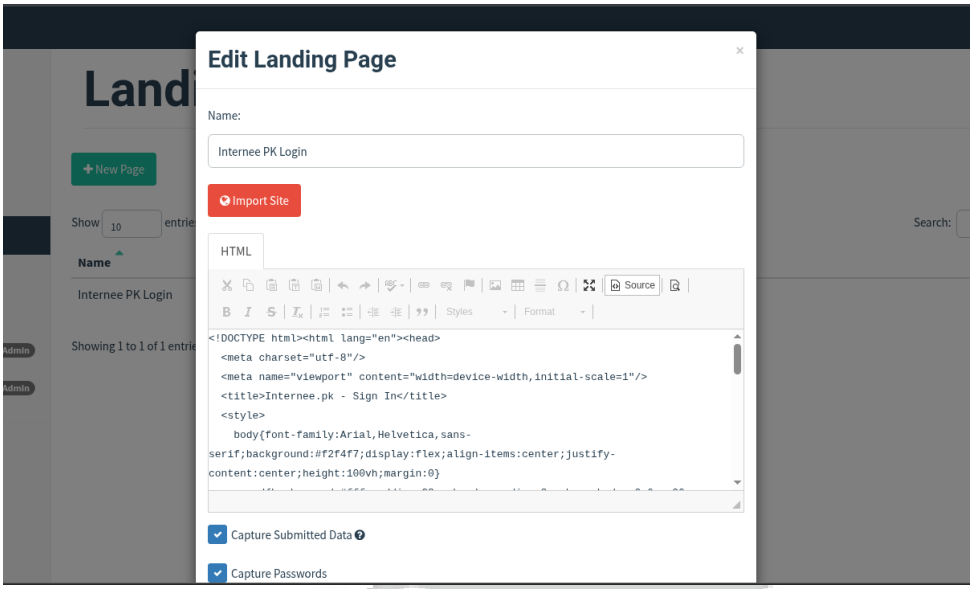


Figure 14: Creating Fake Landing Page. Because the Original Landing Page Cannot be accessible by GoPhish Due to some assets may be blocked, unavailable, or require cookies/headers.

3. **The Phishing Campaign:**

Describe the campaign parameters (targets, email subject, sender name).

- **Target:** axxxs20x3@gmail.com
- **Email Subject**: 'Action Required: Verify Your Internee.pk Account'
- **Sander name:** (axxxs20x3@gmail.com) Choosing same as an example.
- **Snapshot:** The email template or a screenshot of the actual email received.

Email Template:

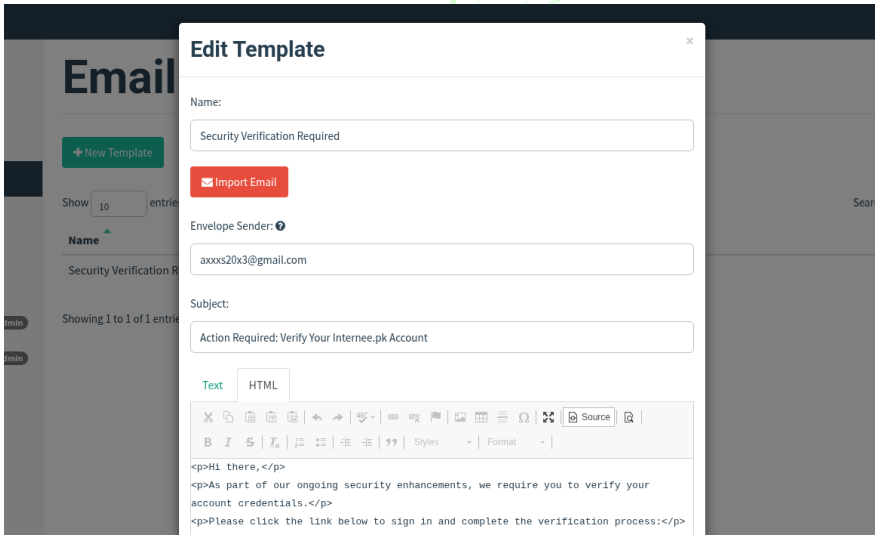


Figure 15: Creating Email Template

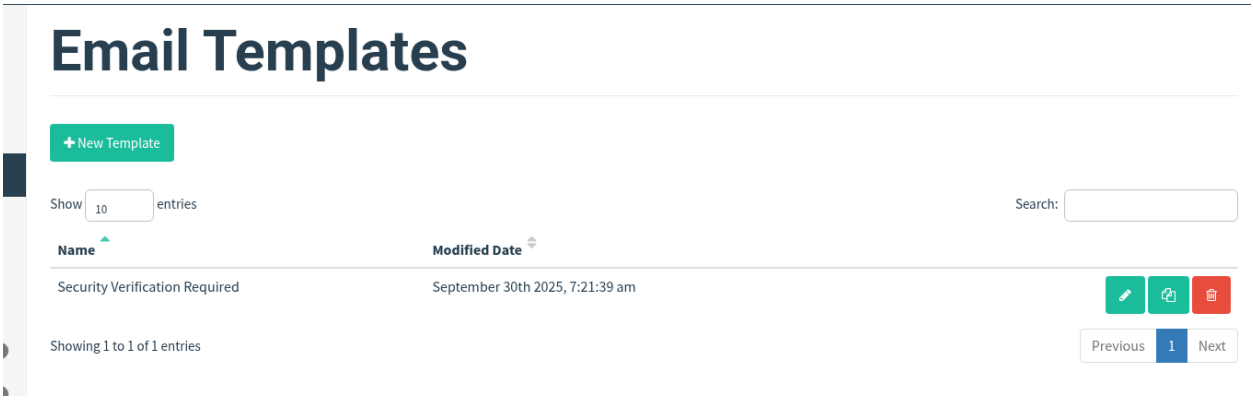


Figure 16: Details of Email template

Email Received:

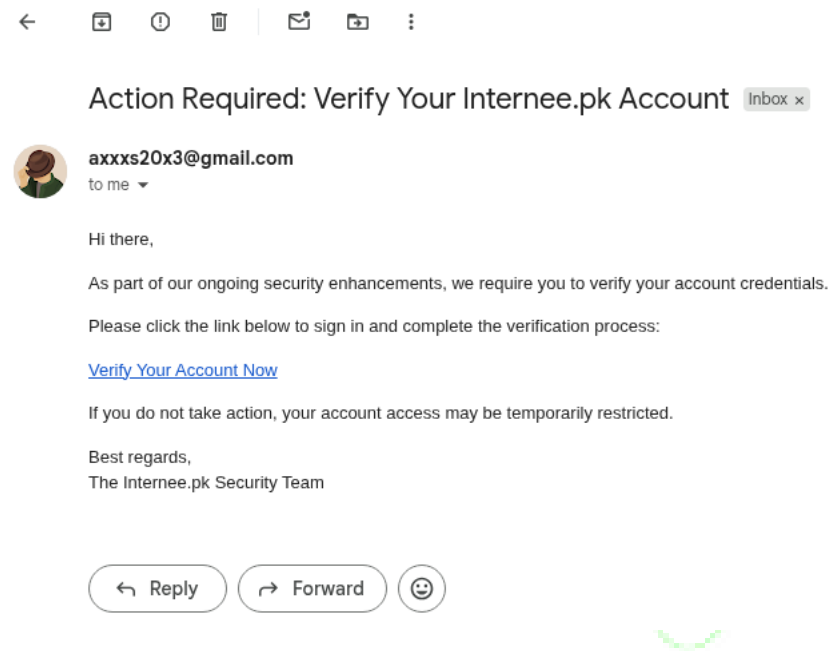


Figure 17: Results: The Phishing Email the user Received after Launching the Campaign

5) Results & Analysis:

The campaign yielded clear and immediate results, demonstrating a full chain of compromise:

METRIC	COUNT	PERCENTAGE	WHAT IT MEANS
EMAILS SENT	1	100%	The campaign was launched successfully.
EMAILS OPENED	1	100%	The subject line was effective in enticing the user to open the email.
CLICKED LINK	1	100%	The user trusted the email content and clicked the phishing link.
SUBMITTED DATA	1	100%	The user entered and submitted their credentials into the fake page.

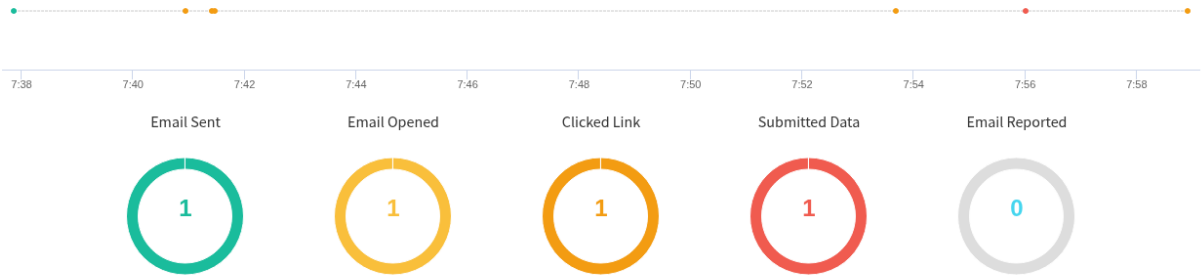


Figure 18: GoPhish results dashboard showing the 100% success rate.

The final campaign results page from GoPhish, showing the captured credentials.

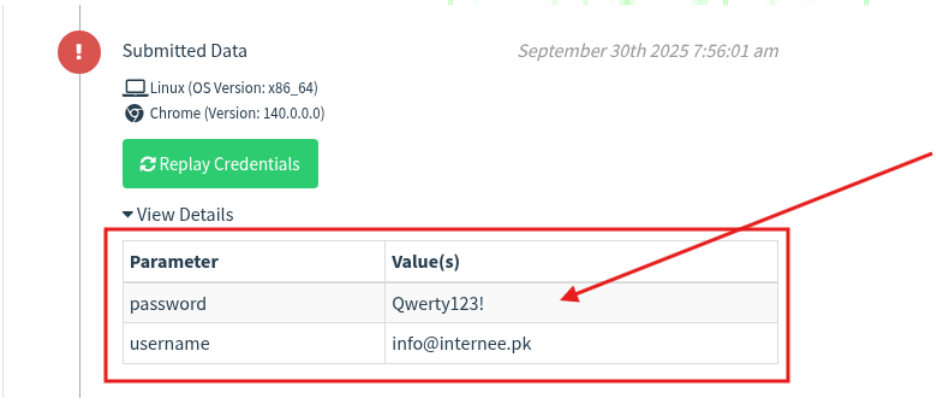


Figure 19: The captured fake credentials submitted by the user.

Analysis:

The 100% success rate, while based on a single test, is a significant finding. It indicates that without specific training, even a basic phishing attempt can bypass individual vigilance. The user proceeded through all stages without hesitation, which in a real-world scenario, would have led to a complete account takeover.

6. In-Depth Security Awareness & Educational Guide

This section is the core of the training derived from this simulation.

6.1. What is Phishing & Social Engineering?

Phishing is a form of social engineering where attackers deceive you into performing an action or revealing information. Social engineering manipulates human psychology—like trust, fear, or curiosity—rather than exploiting technical vulnerabilities. You are the target.

6.2. How to Identify a Phishing Email: Red Flags

Using the simulation email as an example, here are the key red flags to look for:

1. **Sense of Urgency or Threat:** "**Verify now or lose access!"** Legitimate companies rarely use such aggressive tactics.
2. **Generic Greetings:** "**Hi there,"** or "**Dear User**." Most legitimate services from Internee.pk will use your name.
3. **Suspicious Sender Address:** Always check the full email address, not just the display name. Hover your mouse over the "**From**" name to see the real address (e.g., it might reveal axxxs20x3@gmail.com instead of a legitimate **@internee.pk** address).
4. **Mismatched Links:** This is the most critical check. Hover your mouse over any link without clicking it. The true destination **URL** will appear. In our simulation, the link pointed to an IP address (**http://[Kali-IP**]) instead of https://internee.pk .
5. **Requests for Credentials:** A core rule: Legitimate companies will **NEVER** ask you to confirm your password or login via a link in an email.

6.3. Best Practices for Email Security

- **When in Doubt, Don't Click.** If an email seems suspicious, never click links or download attachments.
- **Verify Through Official Channels.** If an email claims to be from Internee.pk IT, contact the IT department directly via a known, trusted method (like a phone number from the company directory) to confirm.
- **Use Strong, Unique Passwords.** This limits the damage if your credentials are ever stolen.
- **Enable Multi-Factor Authentication (MFA):** MFA is a critical second layer of security that can prevent account takeover even if your password is stolen.
- **Report Immediately.** If you suspect a phishing email, report it to your IT/Security team immediately. You are not in trouble for reporting—you are helping protect the company.

7. A Cybersecurity Training Framework for Internee.pk

The results of this simulation make it clear that a one-time training session is insufficient. To build a resilient human firewall, Internee.pk must adopt a continuous, engaging, and modern cybersecurity awareness program. Below is a comprehensive 10-point guideline for training employees in today's digital landscape.

1) Implement a Continuous Learning Cycle, Not Annual Training.

Move away from the outdated "check-the-box" annual training. Adopt a continuous learning model with short, monthly security modules (5-10 minutes) covering topics like phishing, social engineering, password hygiene, and data protection. This keeps security top-of-mind.

2) Deploy Regular, Varied Phishing Simulations.

Use platforms like GoPhish to run quarterly phishing campaigns with varying levels of sophistication. Simulate different attack vectors (e.g., credential harvesting, malware attachments, CEO fraud) and provide immediate, constructive feedback to users who click, explaining what they missed.

3) Gamify the Learning Experience.

Introduce elements of gamification to increase engagement. Create leaderboards for departments with the best phishing report rates, award badges for completing training modules, and run internal "capture-the-flag" challenges related to security. This makes learning competitive and fun.

4) Focus on "Microlearning" Nuggets.

People have short attention spans. Deliver training in bite-sized "nuggets"—short videos, infographics, or interactive quizzes that can be consumed quickly. For example, a 2-minute video deconstructing a recent real-world phishing email is more effective than an hour-long lecture.

5) Conduct Interactive Workshops & Tabletop Exercises.

Host regular workshops where employees can discuss real (anonymized) phishing attempts the company has received. Run tabletop exercises simulating a real security incident (e.g., "What would you do if you lost your laptop?") to build practical incident response skills.

6) Integrate Security into the Company Culture.

Cybersecurity should not be seen as solely IT's responsibility. Leadership must champion security from the top down. Incorporate security reminders into company-wide meetings, newsletters, and internal communication channels like Slack or Teams. Celebrate employees who report phishing attempts.

7) Create a Clear, Simple Reporting Protocol.

Ensure every employee knows exactly how to report a suspicious email. Implement a "Phish Alert Button" (PAB) within the email client (e.g., Outlook) that allows users to report with a single click. Acknowledge and thank employees for their reports to reinforce the behavior.

8) Promote and Enforce Multi-Factor Authentication (MFA).

Training must be backed by robust technology. Mandate the use of MFA on all business-critical applications (email, HR systems, cloud storage). Training should explain why MFA is essential, framing it as a simple step that prevents 99.9% of account compromise attacks, even if a password is stolen.

9) Develop Role-Based Training.

Tailor training content to specific roles. For example, the finance department needs deep training on Business Email Compromise (BEC) and invoice fraud, while HR needs to focus on protecting employee personal data. This makes the training more relevant and impactful.

10) Measure and Adapt the Program.

Track key performance indicators (KPIs) such as phishing click rates, training completion rates, and the number of employee-reported phishing emails. Use this data to measure the program's ROI and adapt the content to address emerging threats and knowledge gaps.

8. Conclusion & Strategic Recommendations

Conclusion:

This phishing simulation served as a stark and valuable wake-up call. The **100%** success rate in credential harvesting demonstrates that sophisticated social engineering attacks pose a clear and present danger to **Internee.pk's** security. While the simulated attack was controlled, it accurately mirrors the tactics used by real threat actors every day. The findings unequivocally show that technological defenses alone are insufficient; the human element is both the primary target and the most critical layer of defense. Therefore, transforming our workforce from a potential vulnerability into a robust "**human firewall**" is not just a recommendation—it is an operational imperative for the company's resilience and security.

Recommendations:

1. **Implement Mandatory Security Awareness Training**: Conduct regular, formal training sessions for all employees, using this report as a case study.
2. **Schedule Regular Phishing Simulations:** Run periodic, controlled simulations with varying difficulty levels to keep security top-of-mind and measure improvement over time.
3. **Promote a "See Something, Say Something" Culture:** Encourage and reward employees for reporting suspicious emails. Ensure the reporting process is simple and well-communicated.
4. **Enforce Strong Password and MFA Policies:** Technically enforce the use of strong passwords and mandate Multi-Factor Authentication on all critical systems.
5. **Disseminate This Report:** Share the findings and educational guide with all staff to kickstart the awareness initiative.

By taking these proactive steps, Internee.pk can significantly reduce its risk profile, protect its valuable assets and reputation, and empower its employees to become active participants in the company's cybersecurity defense.

9. References & Citations

1. Verizon. (2023). 2023 Data Breach Investigations Report. Verizon Business. Retrieved from https://www.verizon.com/business/resources/reports/dbir/
2. KnowBe4. (2023). Phishing By Industry Benchmarking Report. KnowBe4 Research. Retrieved from https://www.knowbe4.com/phishing-by-industry-benchmarking-report
3. CISA. (2021). *Security Tip (ST04-014): Avoiding Social Engineering and Phishing Attacks*. Cybersecurity and Infrastructure Security Agency. Retrieved from https://www.cisa.gov/uscert/ncas/tips/ST04-014
4. GoPhish. (n.d.). Open-Source Phishing Framework. [Computer software]. Retrieved from https://getgophish.com/
5. Proofpoint. (2023). 2023 State of the Phish Report. Proofpoint, Inc. Retrieved from https://www.proofpoint.com/us/resources/threat-reports/state-of-phish