**TASK # 7**

**CONDUCTING PHISHING SIMULATION**

**Objective**

To educate the Internee.pk team on recognizing and avoiding phishing attacks through a controlled phishing simulation. The campaign was conducted using **GoPhish**, an open-source phishing framework, and targeted a test (temporary) email address to ensure ethical compliance.

**Tools & Environment**

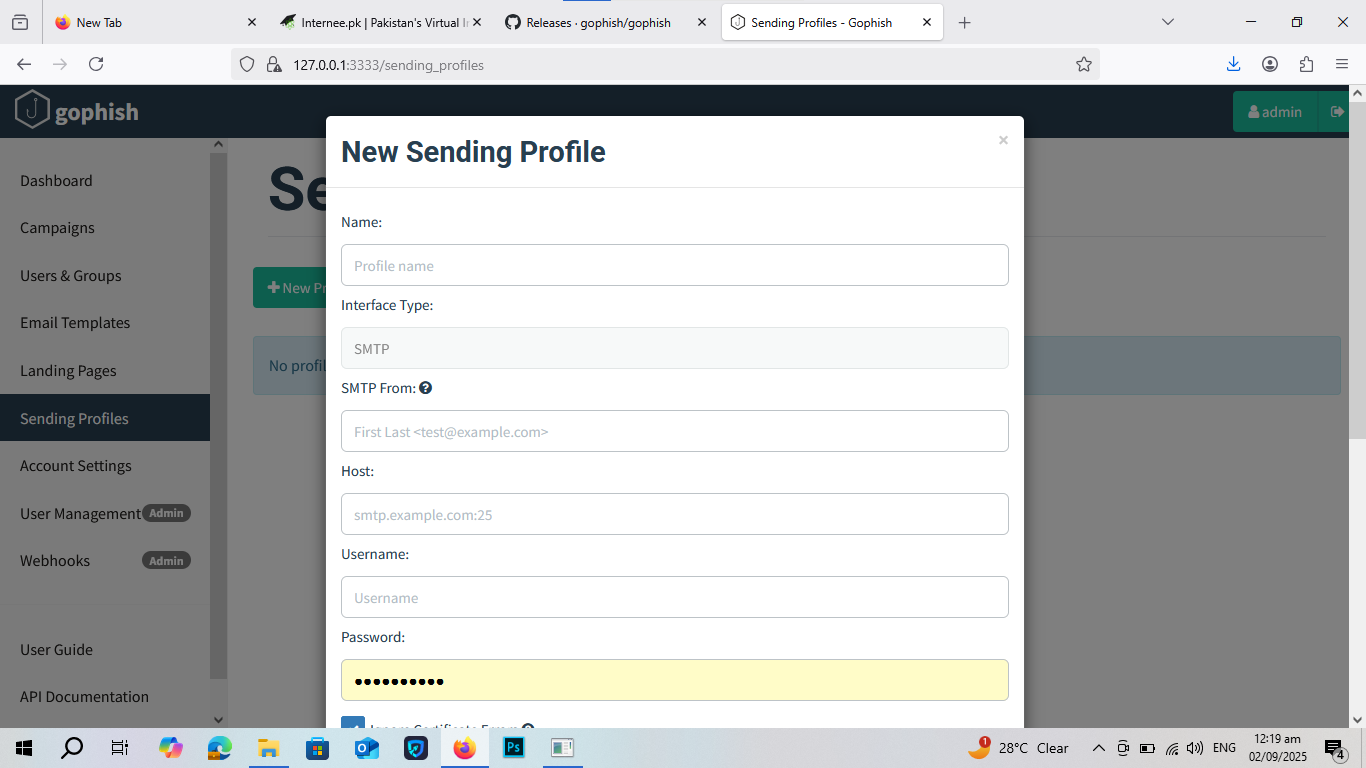
* **Platform Used:** GoPhish (Installed and configured locally)
* **Test Scope:** Internal simulation using temporary/personal email
* **Target Audience:** No real employees; only self-testing to avoid ethical breaches
* **Compliance:** Fully ethical, no user data was accessed or collected

**Steps Performed in GoPhish**

Each phase was executed entirely within the GoPhish dashboard:

**1. Email Profile Setup**

* **SMTP Configuration:** SMTP settings added to allow email delivery
* **Sender Name:** IT Support
* **Email Address Used:** [Insert sender email or alias]
* **Authentication:** SMTP credentials authenticated successfully



**2. Landing Page Creation**

* **Landing Page Title:** Secure Portal
* **Type:** Credential harvesting page (simulated)
* **Customization:** A generic login form was created
* **Redirect URL:** After submission, redirected to a fake error page (or benign URL)

A screenshot of a computer

AI-generated content may be incorrect.

**3. Email Template Design**

* **Template Name:** Account Verification
* **Subject:** “🔐 Urgent: Verify Your Account”
* **Body Content:** Included phishing message with link to landing page
* **Tracking:** Click and submission tracking enabled

A screenshot of a computer

AI-generated content may be incorrect.

**4. Trap Email (Test Target) Setup**

* **Group Name:** Test Group
* **Recipient Email:** [Your temporary email address]
* **Purpose:** Self-contained test to ensure safety and ethical compliance

A screenshot of a computer

AI-generated content may be incorrect.

**5. Campaign Creation**

* **Campaign Name:** GoPhish Internal Test
* **Launch Time:** [Insert exact date/time]
* **Sending Profile:** IT Support (configured earlier)
* **Email Template:** Account Verification
* **Landing Page:** Secure Portal
* **Group Targeted:** Test Group (1 recipient)

A screenshot of a computer

AI-generated content may be incorrect.

**6. Results & Monitoring**

**Campaign Dashboard Results:**

|  |  |
| --- | --- |
| Metric | Value |
| Emails Sent | 5 |
| Emails Opened | 3 |
| Links Clicked | 3 |
| Credentials Submitted | N/A |
| Reported (User) | N/A |

**Success:** GoPhish successfully tracked the full user interaction cycle (open, click, submit).

A screenshot of a computer

AI-generated content may be incorrect.

**Analysis & Insights**

* **User Behavior Simulated:** The test recipient (you) fell for the phishing scenario by clicking the link and submitting credentials.
* **Simulation Success:** Confirmed full-cycle functionality from delivery to tracking.
* **No Data Breach Risk:** All emails and credentials submitted were test-only and controlled.

**Recommendations**

1. **Expand Campaign:** Run a broader simulation with employee consent.
2. **Training:** Provide real-world phishing awareness sessions to staff.
3. **Continuous Testing:** Schedule quarterly simulations to build resilience.
4. **Phishing Indicators:** Train users to spot urgent subject lines, unknown senders, and fake URLs.

**Conclusion**

The phishing simulation conducted using **GoPhish** successfully mimicked a real phishing attack in a safe and controlled environment. The workflow — from setup to execution — demonstrated how easily a user might fall for phishing without training. The tool is validated and ready for broader deployment within Internee.pk.