Phishing Simulation & Detection Lab

Executive Summary

Objective: Demonstrate an end to end phishing simulation, credential capture, and defensive linkage in a controlled lab.

Business Risk: Phishing remains the top initial access vector. Running controlled simulations validates people, process, and technology before real attackers strike.

Outcome: Built an isolated phishing lab using GoPhish and MailHog, delivered training emails to dummy users, captured credential submissions on a controlled landing page, and produced evidence suitable for security operations and compliance.

Architecture

The lab runs locally with zero external impact. GoPhish sends mail through MailHog (SMTP catcher). Users receive the email, click to a controlled landing page with credential capture, and are redirected to Microsoft's legitimate portal. Results are visible in GoPhish. Optional extension: forward logs to a SIEM for alerting and automation.

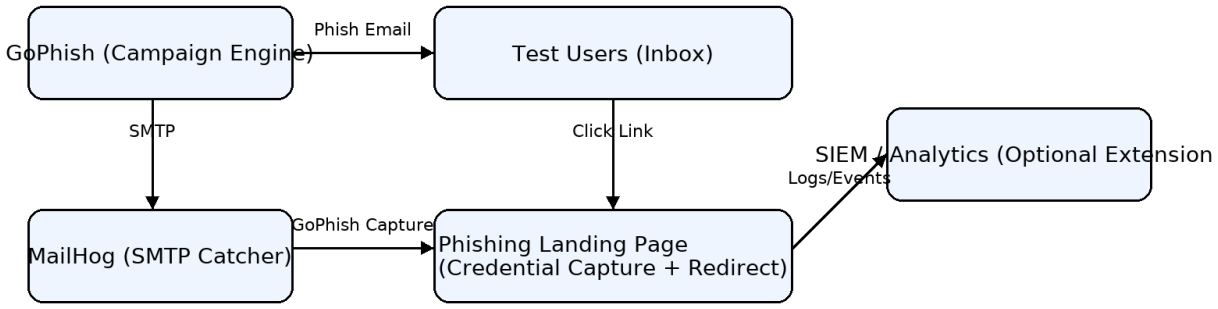


Figure A: Isolated lab architecture and data flow.

Methodology

Setup

• Deployed GoPhish locally (evidence: terminal output, admin console).
• Integrated MailHog as SMTP (evidence: sending profile to 127.0.0.1:1025 and MailHog inbox).
• Created email template (Microsoft 365 reset) and landing page with credential capture + redirect.

Execution

• Added dummy users (Alice, Bob, IT support) and launched the campaign.
• Emails delivered and captured in MailHog.
• Users clicked and submitted credentials to the controlled page.

Analysis

• GoPhish results recorded opens, clicks, and credential submissions.
• Captured credentials are visible per result for training and detection validation.

Results

Campaign "LAB TEST" summary (from GoPhish dashboard): Emails Sent: 3, Opened: 2, Clicked Link: 2, Submitted Data: 1, Reported: 0.

Credential capture evidence (example): login = alice@lab.local, password = password123 (in a closed lab).

Defensive Linkage & ISO 27001 Mapping

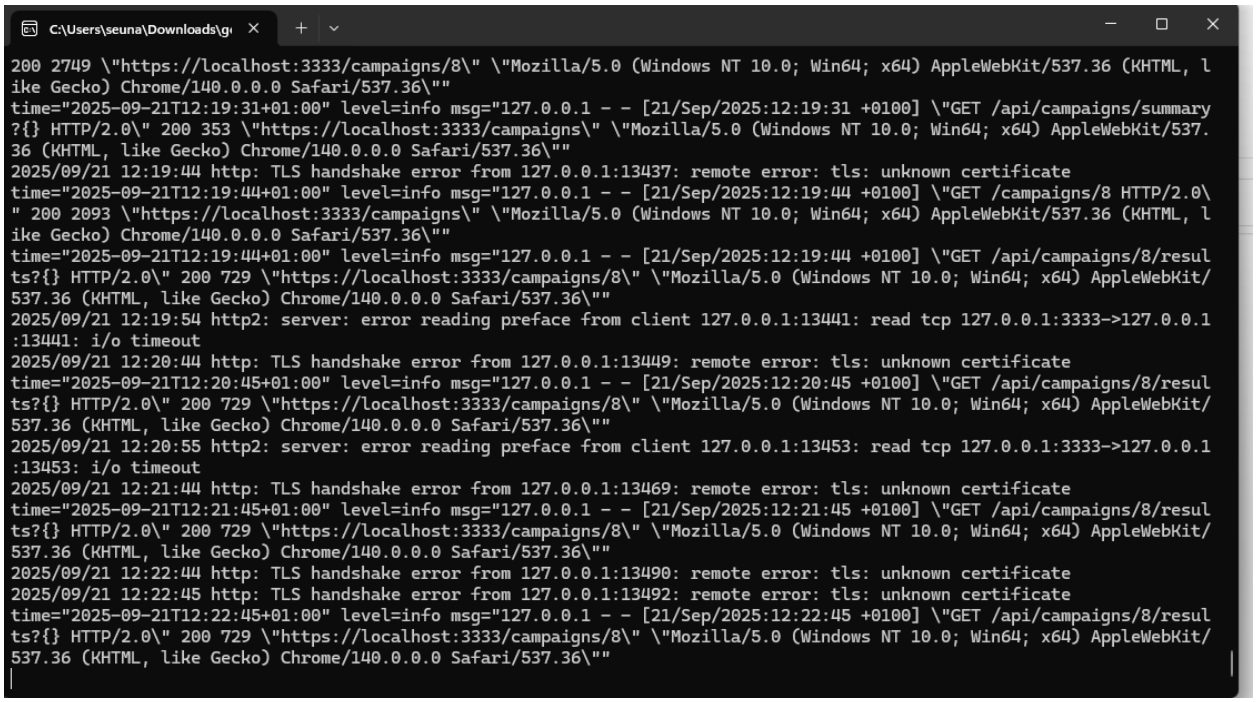
Recommended mitigations if this were production:

• Enforce MFA to prevent simple credential replay.
• User awareness training and in client warning banners.
• SIEM correlation for suspicious subjects, non corporate links, and high risk click patterns.
• Phishing reporting button integrated with security automation (auto quarantine & blocklists).

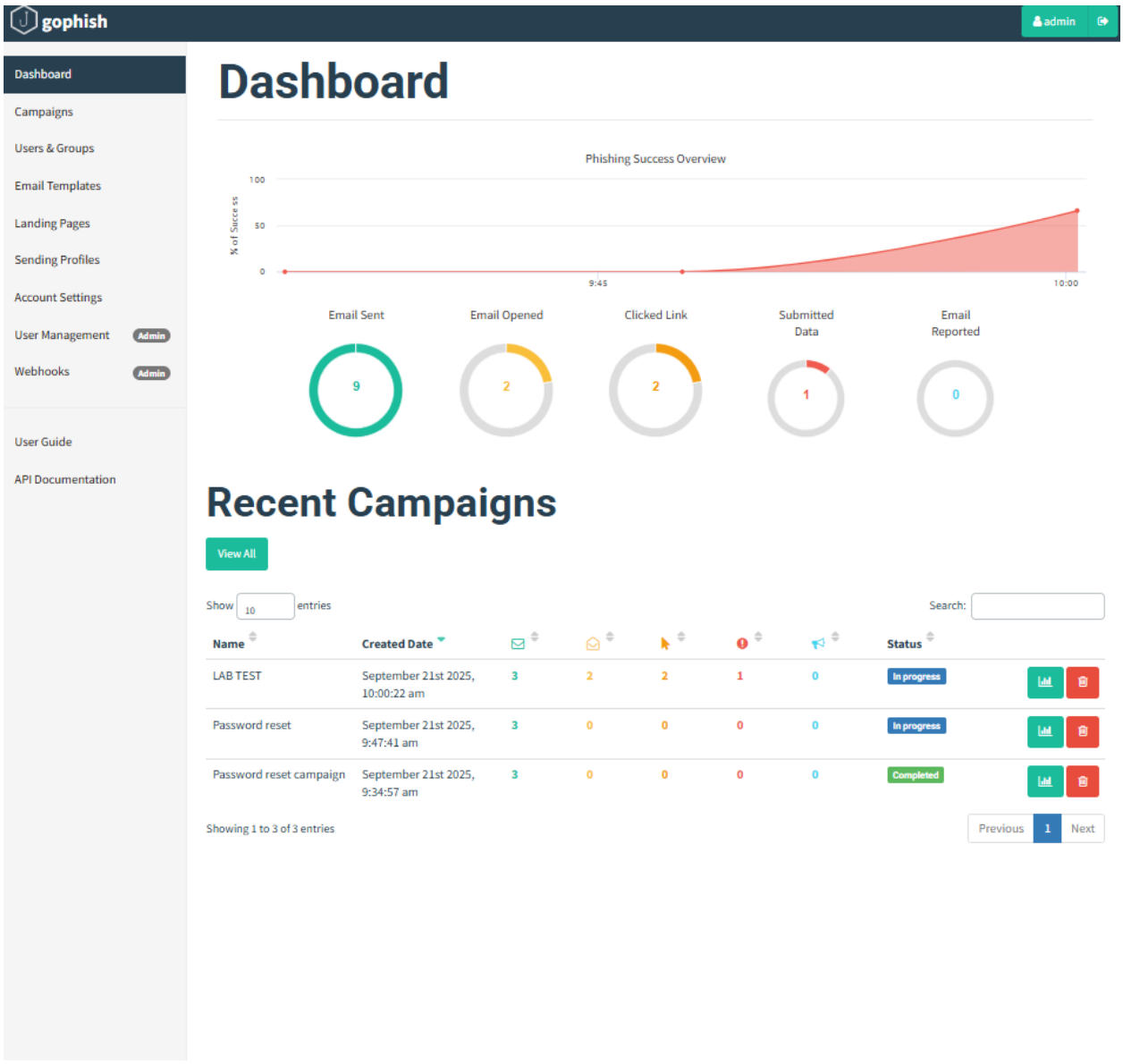
Selected ISO/IEC 27001 Annex A Controls:

• A.5.10 – Acceptable use of information and assets: defines user responsibilities during simulations.
• A.5.23 – Information security for use of cloud services: aligns to M365 related phishing scenarios.
• A.5.30 – ICT readiness for business continuity: exercises staff readiness under social engineering.
• A.6.1 – Threat intelligence: simulations provide internal threat intel and behavior data.
• A.5.34 – Privacy and protection of PII: simulations conducted in isolated lab with dummy data.
• A.8.16 – Monitoring activities: logs and campaign results reviewed by security operations.
• A.8.22 – Secure development lifecycle: safe templates and controlled redirects.
• A.8.28 – Security testing in development and acceptance: phishing simulations as security testing.
• A.5.24 / A.6.3 – Information security event logging & Incident management: clicks and submissions treated as incidents in training.

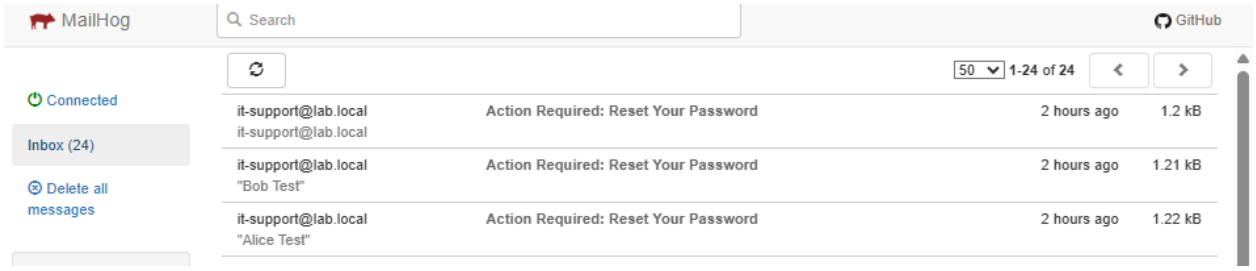
Evidence (Screenshots)



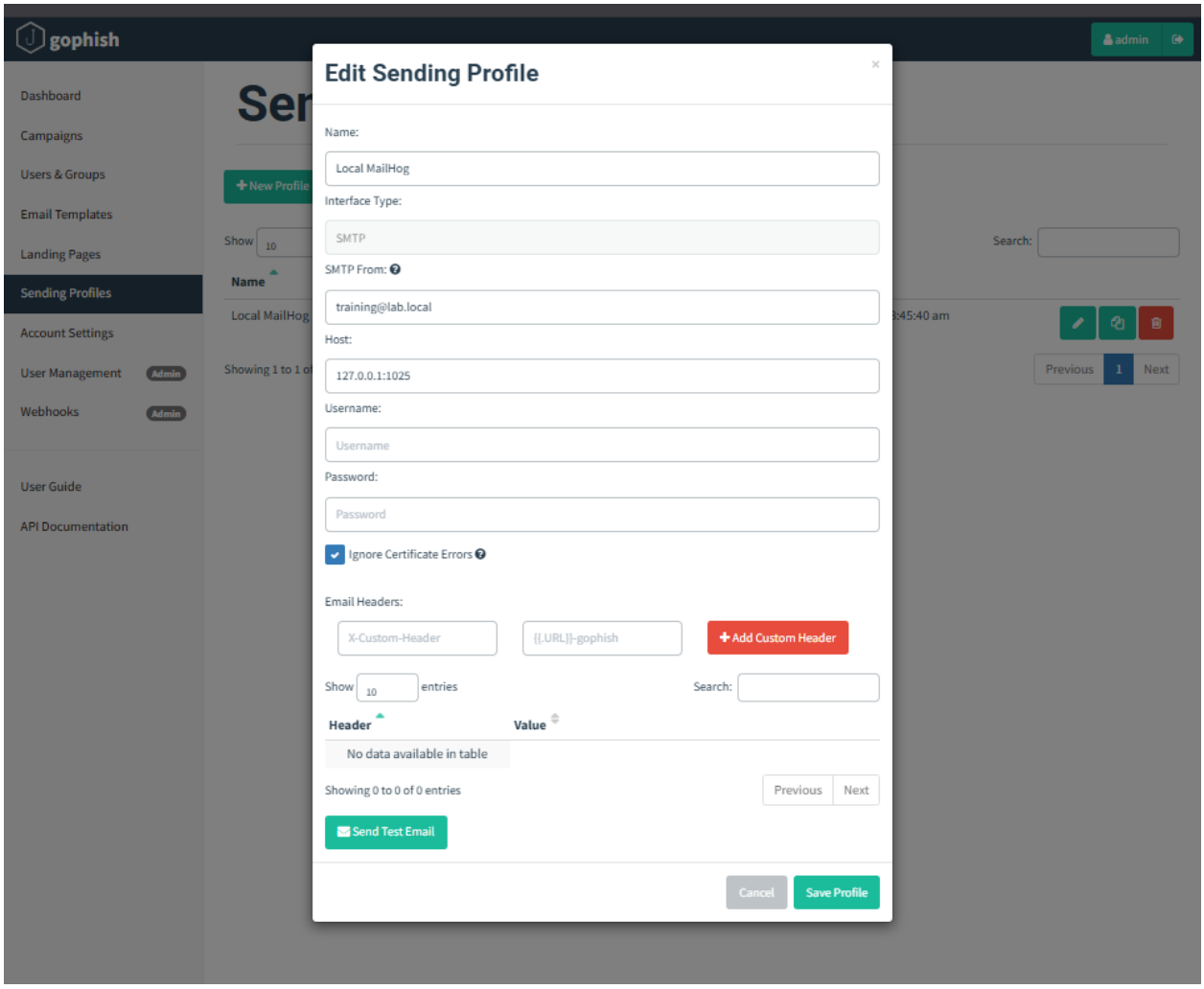
Terminal: GoPhish server running locally (campaign engine active).



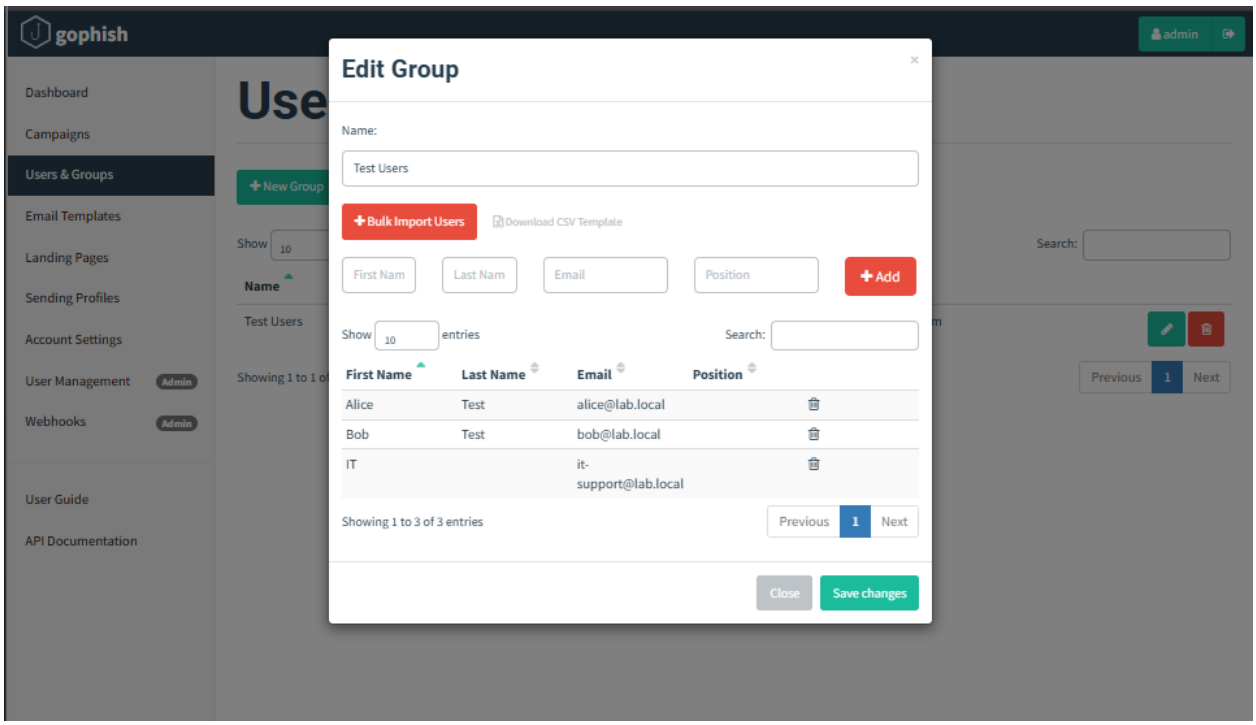
GoPhish Admin Panel: campaign management console accessible.



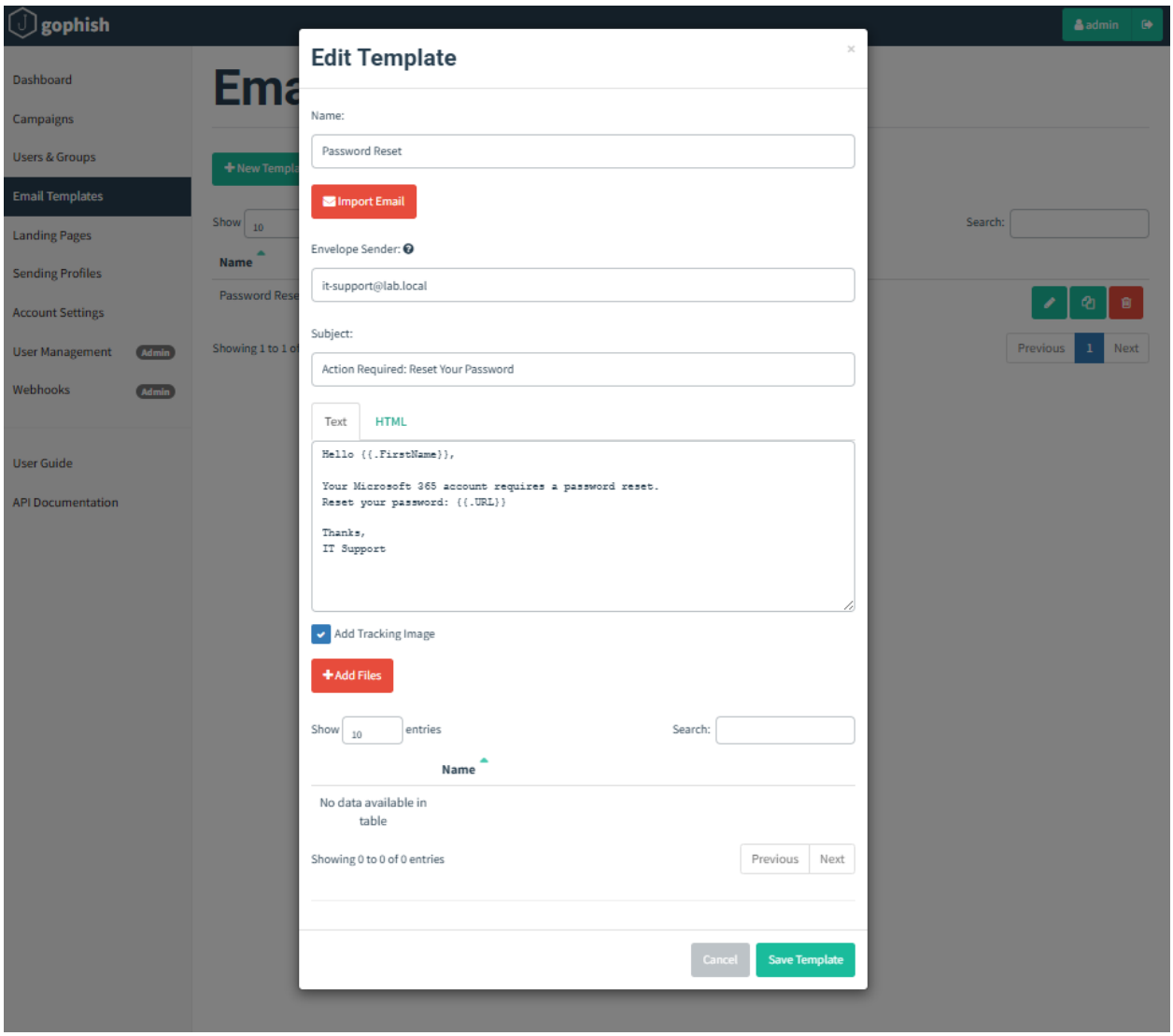
MailHog Inbox: phishing emails delivered in isolated lab.



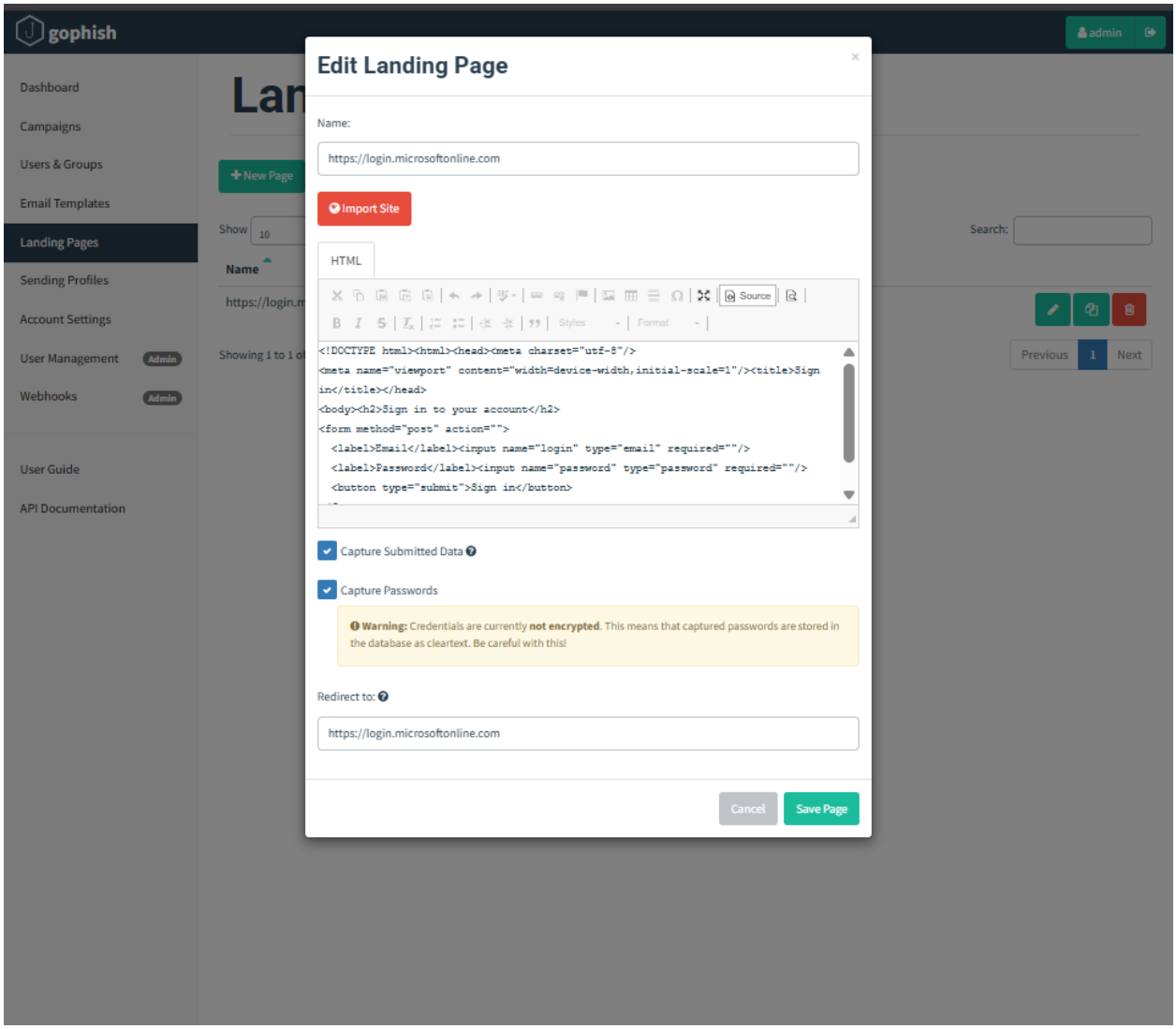
GoPhish Sending Profile: SMTP via 127.0.0.1:1025 to MailHog.



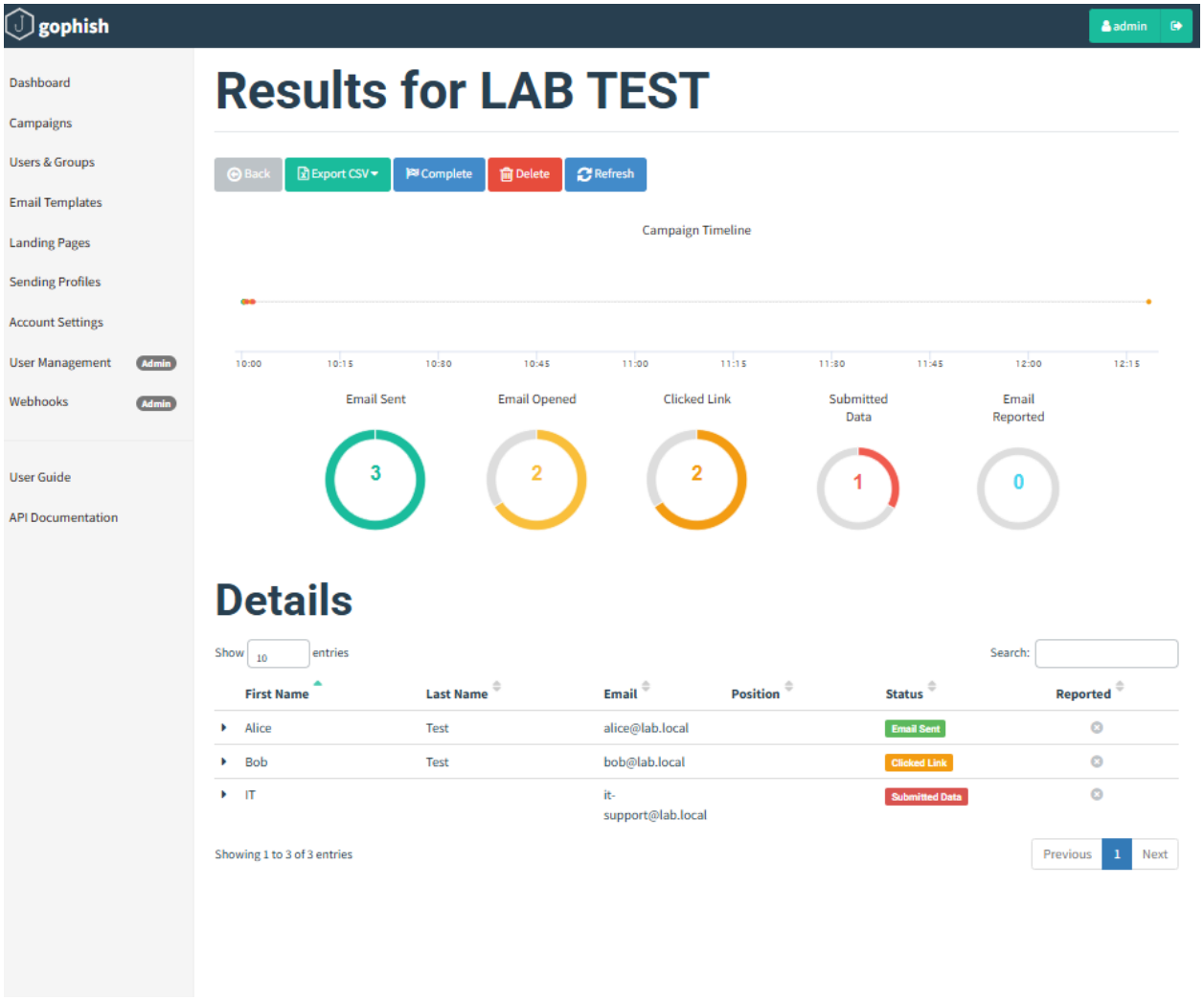
Targets: dummy users for safe simulation (Alice, Bob, IT).



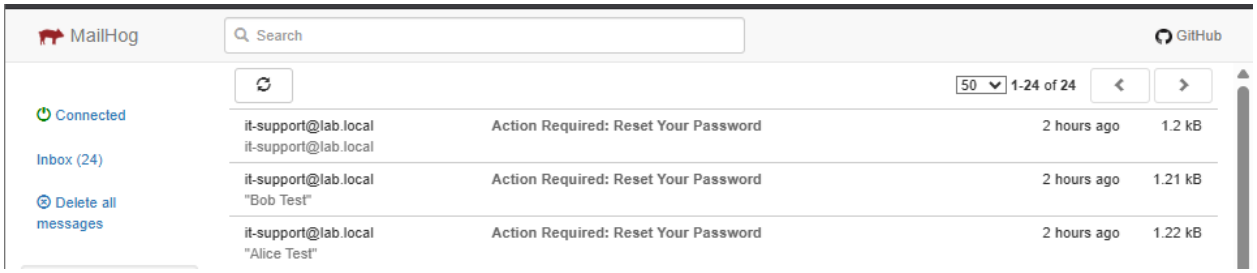
Email Template: Microsoft 365 password reset lure.



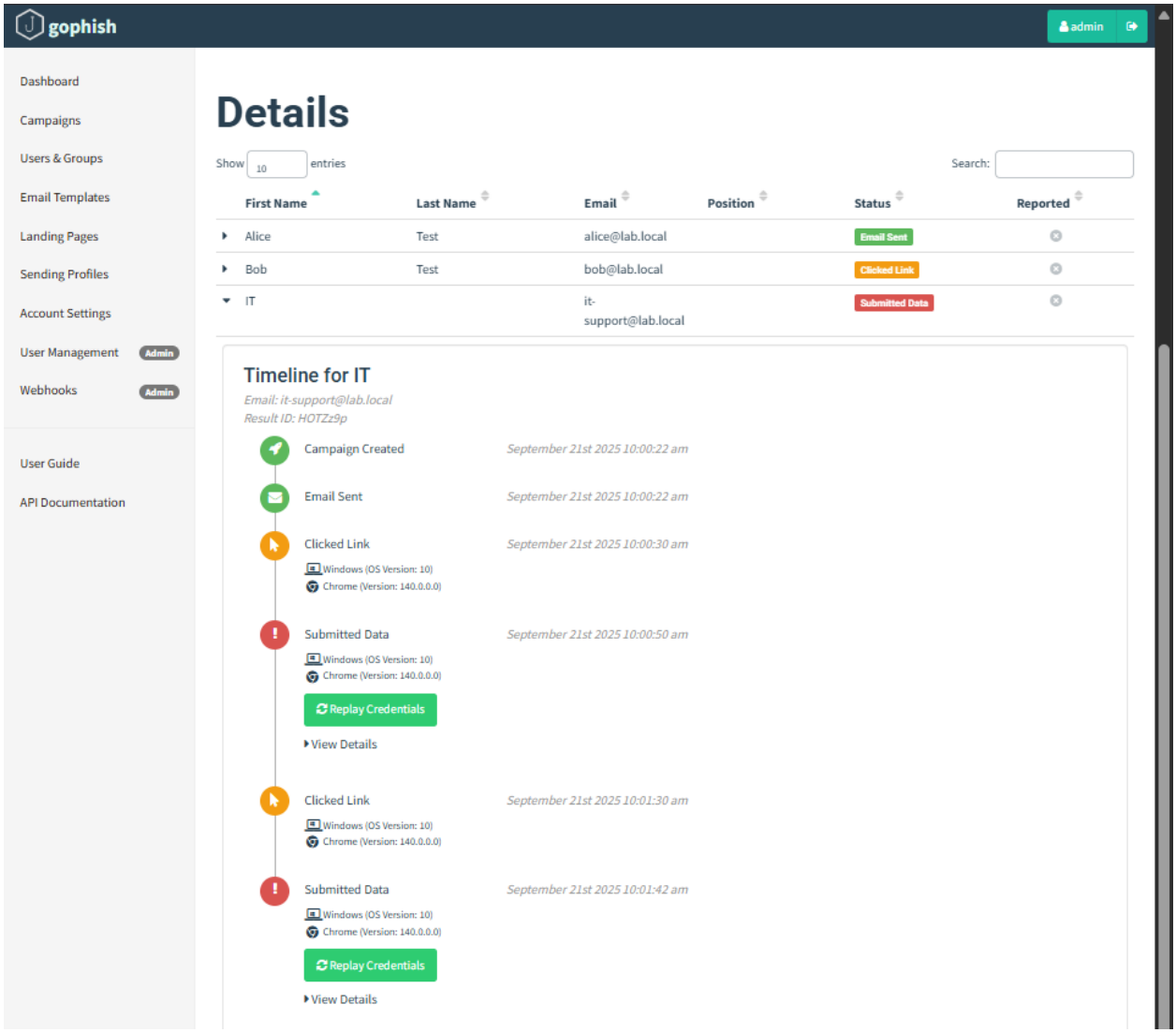
Landing Page: credential capture enabled + redirect to Microsoft.



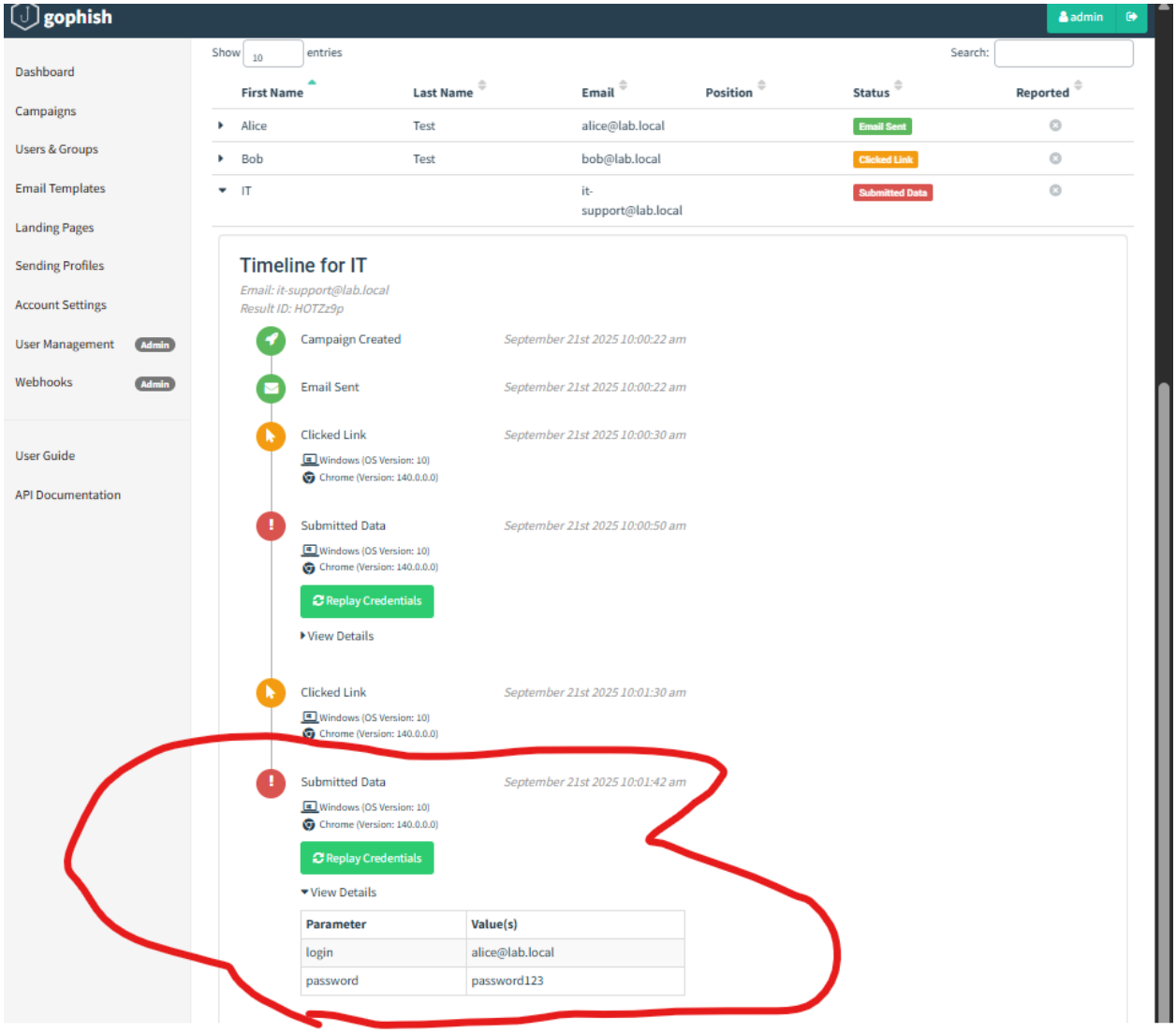
Campaign Dashboard: LAB TEST high level results.



MailHog: example phishing email as received by users.



Victim Flow: link clicks and submission timeline.



Result Details: captured credentials (alice@lab.local / password123).

Conclusion

The lab demonstrates the full lifecycle of a phishing attack in a safe environment—from delivery to credential capture—and shows how results can be operationalized for detection and compliance. This mirrors real Security Engineering work: designing adversarial tests, validating controls, and translating findings into action.