

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.

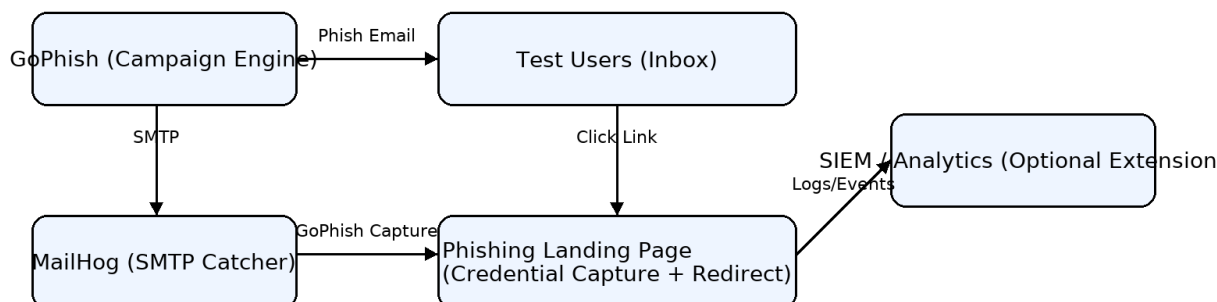


Figure A: Isolated lab architecture and data flow.

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).

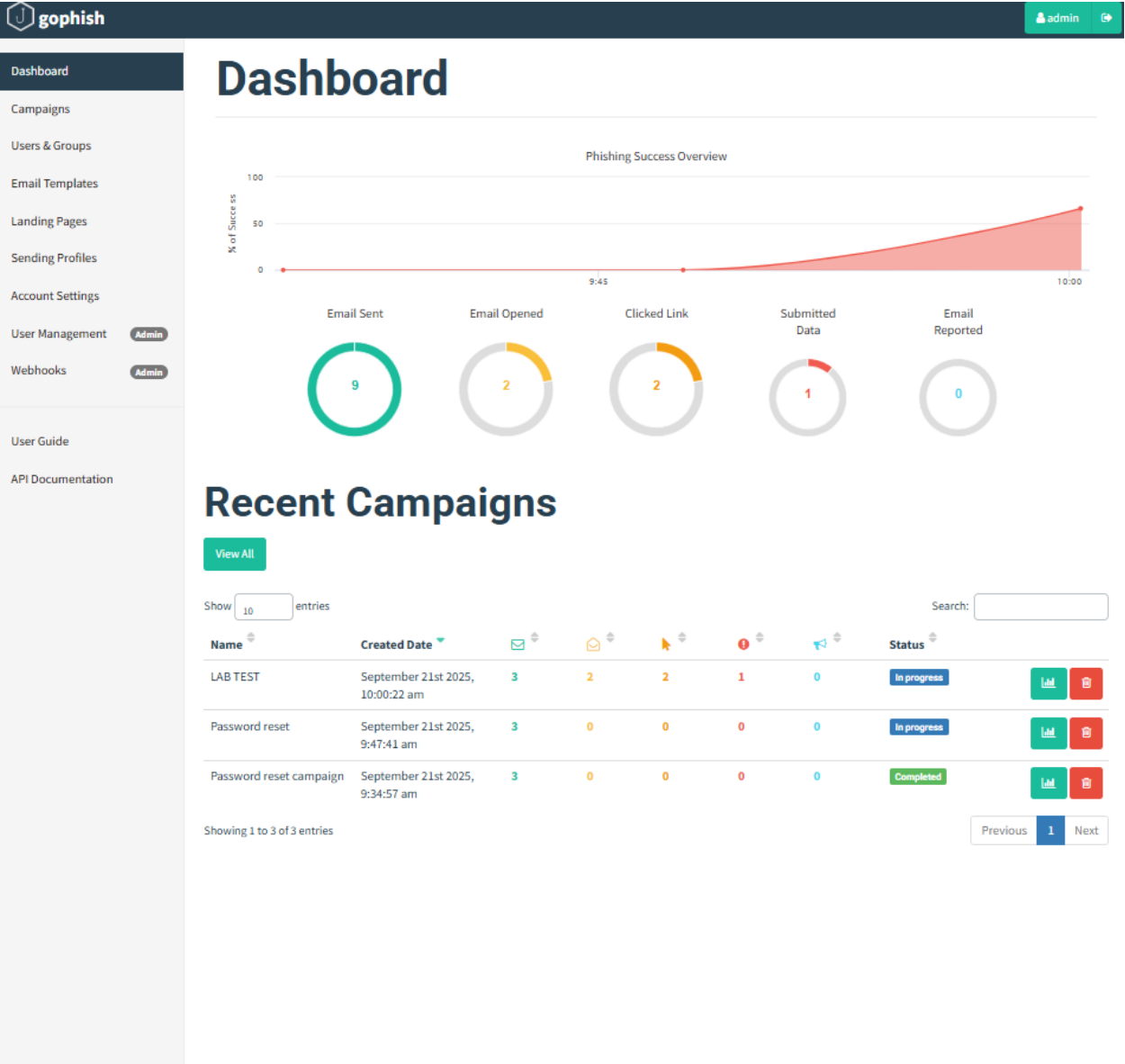
Selected ISO/IEC 27001 Annex A Controls:

- 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)

```
C:\Users\seuna\Downloads\g... X + -
200 2749 \"https://localhost:3333/campaigns/8\" \"Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/140.0.0.0 Safari/537.36\"
time=\"2025-09-21T12:19:31+01:00\" level=info msg=\"127.0.0.1 - - [21/Sep/2025:12:19:31 +0100] \\\"GET /api/campaigns/summary?{} HTTP/2.0\\\" 200 353 \\\"https://localhost:3333/campaigns/8\\\" \"Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/140.0.0.0 Safari/537.36\\\"\"
2025/09/21 12:19:44 http: TLS handshake error from 127.0.0.1:13437: remote error: tls: unknown certificate
time=\"2025-09-21T12:19:44+01:00\" level=info msg=\"127.0.0.1 - - [21/Sep/2025:12:19:44 +0100] \\\"GET /campaigns/8 HTTP/2.0\\\" 200 2093 \\\"https://localhost:3333/campaigns/8\\\" \"Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/140.0.0.0 Safari/537.36\\\"\"
time=\"2025-09-21T12:19:44+01:00\" level=info msg=\"127.0.0.1 - - [21/Sep/2025:12:19:44 +0100] \\\"GET /api/campaigns/8/results?{} HTTP/2.0\\\" 200 729 \\\"https://localhost:3333/campaigns/8\\\" \"Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/140.0.0.0 Safari/537.36\\\"\"
2025/09/21 12:19:54 http2: server: error reading preface from client 127.0.0.1:13441: read tcp 127.0.0.1:3333->127.0.0.1:13441: i/o timeout
2025/09/21 12:20:44 http: TLS handshake error from 127.0.0.1:13449: remote error: tls: unknown certificate
time=\"2025-09-21T12:20:45+01:00\" level=info msg=\"127.0.0.1 - - [21/Sep/2025:12:20:45 +0100] \\\"GET /api/campaigns/8/results?{} HTTP/2.0\\\" 200 729 \\\"https://localhost:3333/campaigns/8\\\" \"Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/140.0.0.0 Safari/537.36\\\"\"
2025/09/21 12:20:55 http2: server: error reading preface from client 127.0.0.1:13453: read tcp 127.0.0.1:3333->127.0.0.1:13453: i/o timeout
2025/09/21 12:21:44 http: TLS handshake error from 127.0.0.1:13469: remote error: tls: unknown certificate
time=\"2025-09-21T12:21:45+01:00\" level=info msg=\"127.0.0.1 - - [21/Sep/2025:12:21:45 +0100] \\\"GET /api/campaigns/8/results?{} HTTP/2.0\\\" 200 729 \\\"https://localhost:3333/campaigns/8\\\" \"Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/140.0.0.0 Safari/537.36\\\"\"
2025/09/21 12:22:44 http: TLS handshake error from 127.0.0.1:13490: remote error: tls: unknown certificate
2025/09/21 12:22:45 http: TLS handshake error from 127.0.0.1:13492: remote error: tls: unknown certificate
time=\"2025-09-21T12:22:45+01:00\" level=info msg=\"127.0.0.1 - - [21/Sep/2025:12:22:45 +0100] \\\"GET /api/campaigns/8/results?{} HTTP/2.0\\\" 200 729 \\\"https://localhost:3333/campaigns/8\\\" \"Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/140.0.0.0 Safari/537.36\\\"\"
```

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



gophish

Dashboard

Campaigns

Users & Groups

Email Templates

Landing Pages

Sending Profiles

Account Settings

User Management Admin

Webhooks Admin

User Guide

API Documentation

Send

+ New Profile

Show 10

Name

Local MailHog

Showing 1 to 1 of 1 entries

Search:

Previous 1 Next

Edit Sending Profile

×

Name:

Local MailHog

Interface Type:

SMTP

SMTP From:

training@lab.local

Host:

127.0.0.1:1025

Username:

Username

Password:

Password

☒ Ignore Certificate Errors

Email Headers:

X-Custom-Header

{{URL}}-gophish

+ Add Custom Header

Show 10 entries

Search:

Header

Value

No data available in table

Showing 0 to 0 of 0 entries

Previous Next

Send Test Email

Cancel

Save Profile

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

gophish

Dashboard

Campaigns

Users & Groups

Email Templates

Landing Pages

Sending Profiles

Account Settings

User Management Admin

Webhooks Admin

User Guide

API Documentation

User

+ New Group

Show 10

Name

Test Users

Showing 1 to 1 of 1 entries

Search:

Previous 1 Next

Edit Group

×

Name:

Test Users

+ Bulk Import Users

Download CSV Template

First Name

Last Name

Email

Position

+ Add

Show 10 entries

Search:

First Name

Last Name

Email

Position

Alice

Test

alice@lab.local

Bob

Test

bob@lab.local

IT

it-support@lab.local

Showing 1 to 3 of 3 entries

Previous 1 Next

Close

Save changes

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

Edit Template

Name: Password Reset

[Import Email](#)

Envelope Sender: [it-support@lab.local](#)

Subject: Action Required: Reset Your Password

Text **HTML**

Hello {{.FirstName}},

Your Microsoft 365 account requires a password reset.
Reset your password: {{.URL}}

Thanks,
IT Support

☒ Add Tracking Image

[+ Add Files](#)

Show 10 entries Search:

Name

No data available in table

Showing 0 to 0 of 0 entries Previous Next

Cancel Save Template

Email Template: Microsoft 365 password reset lure.

gophish

admin

Dashboard

Campaigns

Users & Groups

Email Templates

Landing Pages

Sending Profiles

Account Settings

User Management **Admin**

Webhooks **Admin**

User Guide

API Documentation

+ New Page

Show 10

Name

https://login.m

Showing 1 to 1 of 1

Search:

Previous 1 Next

Edit Landing Page

Name:

https://login.microsoftonline.com

Import Site

HTML

```
<!DOCTYPE html><html><head><meta charset="utf-8"/>
<meta name="viewport" content="width=device-width,initial-scale=1"/><title>Sign
in</title></head>
<body><h2>Sign in to your account</h2>
<form method="post" action="">
  <label>Email</label><input name="login" type="email" required="">
  <label>Password</label><input name="password" type="password" required="">
  <button type="submit">Sign in</button>
</form>
```

☒ Capture Submitted Data

☒ Capture Passwords

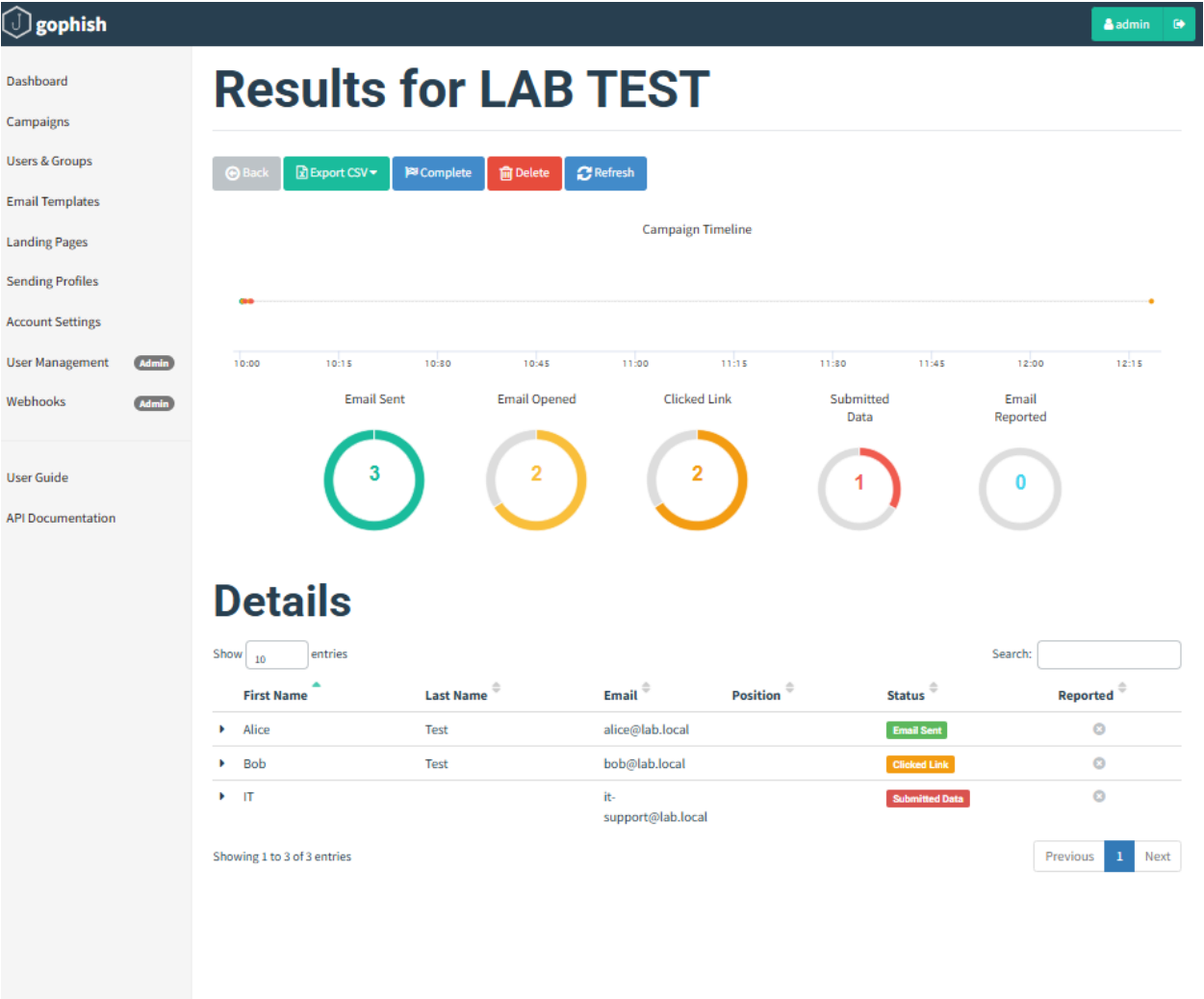
Warning: Credentials are currently **not encrypted**. This means that captured passwords are stored in the database as cleartext. Be careful with this!

Redirect to:

https://login.microsoftonline.com

Cancel Save Page

Landing Page: credential capture enabled + redirect to Microsoft.



Campaign Dashboard: LAB TEST high level results.

MailHog Search GitHub

50 1-24 of 24

Connected	it-support@lab.local	Action Required: Reset Your Password	2 hours ago	1.2 kB
Inbox (24)	it-support@lab.local	Action Required: Reset Your Password	2 hours ago	1.21 kB
Delete all messages	it-support@lab.local	Action Required: Reset Your Password	2 hours ago	1.22 kB

MailHog: example phishing email as received by users.

admin

Dashboard

Campaigns

Users & Groups

Email Templates

Landing Pages

Sending Profiles

Account Settings

User ManagementAdmin

WebhooksAdmin

User Guide

API Documentation

Details

Show 10 entries

Search:

First Name	Last Name	Email	Position	Status	Reported
Alice	Test	alice@lab.local		Email Sent	
Bob	Test	bob@lab.local		Clicked Link	
IT		it-support@lab.local		Submitted Data	

Timeline for IT

Email: it-support@lab.local

Result ID: HOTZz9p

Campaign Created

September 21st 2025 10:00:22 am

Email Sent

September 21st 2025 10:00:22 am

Clicked Link

September 21st 2025 10:00:30 am

Windows (OS Version: 10)

Chrome (Version: 140.0.0.0)

Submitted Data

September 21st 2025 10:00:50 am

Windows (OS Version: 10)

Chrome (Version: 140.0.0.0)

Replay Credentials

View Details

Clicked Link

September 21st 2025 10:01:30 am

Windows (OS Version: 10)

Chrome (Version: 140.0.0.0)

Submitted Data

September 21st 2025 10:01:42 am

Windows (OS Version: 10)

Chrome (Version: 140.0.0.0)

Replay Credentials

View Details

Victim Flow: link clicks and submission timeline.

gophish

admin

Show 10 entries

Search:

First Name	Last Name	Email	Position	Status	Reported
Alice	Test	alice@lab.local		Email Sent	
Bob	Test	bob@lab.local		Clicked Link	
IT		it-support@lab.local		Submitted Data	

Timeline for IT

Email: it-support@lab.local

Result ID: HOTZz9p

Campaign Created

September 21st 2025 10:00:22 am

Email Sent

September 21st 2025 10:00:22 am

Clicked Link

September 21st 2025 10:00:30 am

Windows (OS Version: 10)

Chrome (Version: 140.0.0.0)

Submitted Data

September 21st 2025 10:00:50 am

Windows (OS Version: 10)

Chrome (Version: 140.0.0.0)

Replay Credentials

View Details

Clicked Link

September 21st 2025 10:01:30 am

Windows (OS Version: 10)

Chrome (Version: 140.0.0.0)

Submitted Data

September 21st 2025 10:01:42 am

Windows (OS Version: 10)

Chrome (Version: 140.0.0.0)

Replay Credentials

View Details

Parameter	Value(s)
login	alice@lab.local
password	password123

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.