Incident Response Simulation Report

Simulation: Phishing Email (MailHog)

Name: Khaled Gamal Abdelhalim
ID: 2201562
Date of simulation: October 28, 2025

1. Incident Description

Type of attack: Phishing email attack (MailHog test environment)

Objective: Test the Incident Response Team (IRT) readiness to detect and document a phishing email targeting internal/test accounts. Collect logs and artifacts and produce a timeline for analysis.

2. Simulation Scenario

How the malicious email was sent:

- The phishing messages were generated and injected into the MailHog SMTP service from a test machine (kali) using a phishing tool (gophish header observed).
- Sender: `training@lab.local` (MAIL FROM). MailHog stored messages and provided unique message IDs.
- Recipients used in the simulation: `123hhkhaled@gmail.com` and `kgg900014@gmail.com`.

Email content (rendered text):

```
Subject: Security_Training – Please_Read

Hi Khaled,

Our security systems detected suspicious activity on your account.
To ensure your access remains secure we require a brief verification.

Please click the button below to reset and confirm your account:

Reset your password: http://192.168.159.130?rid=JZKrRyr

If the button does not work, copy and paste this link into your browser:
http://192.168.159.130?rid=JZKrRyr

Regards,
IT Support
```

The message used HTML formatting and included a hidden tracking image referencing `http://192.168.159.130/track?rid=…`.

How it was received on the server (MailHog):

- SMTP session began from `127.0.0.1:52982`. EHLO, AUTH PLAIN and MAIL FROM / RCPT TO / DATA sequence executed.

- MailHog reported stored message IDs, e.g. `P1CfMUPkFhehkFxm5n5Y6eYXcdoWfuThbbPCcKyfgI8=` and `5iyiIeyATdKO_DqgruA1I0GCaYu4FlJM6SvBDFBo6FU=`.
- No links were clicked and no attachments were executed — the simulation was passive to avoid harm.

3. Collected Evidence

Evidence Type	Description / Suggested Filename
Server SMTP logs	`mailhog_smtp_session_logs.txt` — full captured SMTP session (timestamps, commands, responses)
Raw email (EML)	`phishing_email_\.eml` — the complete raw message as stored by MailHog
Email headers	`phishing_email_headers.txt` — parsed headers (From, To, Subject, Message-ID, X-Mailer, Received, Content-Type)
Email body (HTML)	`phishing_email_body.html` — the HTML body extracted from the message
Suspicious URLs	`suspicious_urls.txt` — e.g. `http://192.168.159.130?rid=JZKrRyr`
Screenshots	`mailhog_list_view.png`, `mailhog_message_view.png` — screenshots of MailHog UI showing received messages
Message IDs / metadata	Stored IDs and creation times (see timeline and raw JSON exported from MailHog)

Note: Keep all evidence files read-only and preserve original timestamps. If moving files, compute and store cryptographic hashes (SHA256) for chain-of-custody integrity.

4. Example Email Headers (extracted)

```
From: 123hhkhaled@gmail.com
To: "Khaled ali" <123hhkhaled@gmail.com>
Subject: =?UTF-8?q?Security_Training_=E2=80=94_Please_Read?=
Message-ID: <1761693266404372881.8666.283763266971654988l@kali>
Date: Tue, 28 Oct 2025 19:14:26 -0400
X-Mailer: gophish
Return-Path: <training@lab.local>
Received: from kali by mailhog.example (MailHog)
Content-Type: text/html; charset=UTF-8
Content-Transfer-Encoding: quoted-printable
```

(Full headers available in the `phishing_email_headers.txt` artifact.)

5. Timeline (detailed)

Timestamp (local)	Event
2025-10-28 19:14:26	SMTP session started from 127.0.0.1:52982 (MailHog) — Server sent greeting: `220 mailhog.example ESMTP MailHog`
2025-10-28 19:14:26	Client: `EHLO kali` — server responded with capabilities and switched to MAIL state
2025-10-28 19:14:26	AUTH PLAIN performed; server accepted authentication: `235 Authentication successful`
2025-10-28 19:14:26	MAIL FROM: <training@lab.local> — server acknowledged sender
2025-10-28 19:14:26	RCPT TO: <123hhkhaled@gmail.com> — recipient accepted
2025-10-28 19:14:26	DATA command received; SMTP client transmitted HTML message body; server stored message with ID `P1CfMUPkFhehkFxm5n5Y6eYXcdoWfuThbbPCcKyfgI8=@mailhog.example`
2025-10-28 19:14:26	Second RCPT TO: <kgg900014@gmail.com> and second DATA transaction — message stored with ID `5iyiIeyATdKO_DqgruA1I0GCaYu4FlJM6SvBDFBo6FU=@mailhog.example`
2025-10-28 19:14:26	Client sent QUIT; session ended (server replied `221 Bye`)

All timestamps taken from MailHog SMTP logs and MailHog API JSON export. No link clicks or attachments were executed during this simulation.

6. Analysis & Observations

- The email sender was forged (From header is `123hhkhaled@gmail.com`) while MAIL FROM is `training@lab.local` — typical of phishing tests.
- X-Mailer indicates a phishing tool (header `X-Mailer: gophish`), which helps identify the campaign origin in a test environment.
- Message contains a tracking image pointing at `http://192.168.159.130/track?rid=…` — useful to detect recipient engagement if the simulation had included click/exfiltration steps.
- Because messages were captured by MailHog (test sink), the risk to real users was mitigated; however, same indicators would appear in production environments and should trigger detection rules.

7. Recommended Next Steps

1. Preserve all evidence files in a secure location and compute hashes (SHA256) for each artifact.
2. Import the raw EML into a mail analysis tool (or MTA logs) for deeper header/trail analysis.
3. Create or tune email gateway detection rules blocking IPs/URLs and flagging `X-Mailer: gophish` or similar indicators.

4. Run a controlled click/test of the link in a fully isolated sandbox to observe potential payloads or redirect behavior (only after approvals).
5. Perform Lessons Learned session with IRT and update IR playbook to include this phishing pattern and detection play.

8. Attachments & Evidence Index

Attach the following files to the case folder (make them read-only after collection):

- `mailhog_smtp_session_logs.txt` — full SMTP session log (raw)
- `phishing_email_<MessageID>.eml` — raw EML
- `phishing_email_headers.txt` — parsed headers
- `phishing_email_body.html` — extracted HTML body
- `suspicious_urls.txt` — list of extracted URLs with notes
- Screenshots: `mailhog_list_view.png`, `mailhog_message_view.png`
- Hashes: `evidence_hashes.txt` — SHA256 hashes for each file

Prepared by Incident Response Simulation Team — Document version 1.0 • Generated: 2025-10-28