Phishing Incident Response Playbook
Version: 1.0
Owner: Information Security
Company: Gladden Tech (Sample Organization)
Last Updated: 2025-01-01

1. Purpose
This playbook outlines the required steps for detecting, analyzing, containing, eradicating, and recovering from phishing incidents. Its goal is to minimize impact, protect company data, and ensure a consistent, repeatable response to email-based threats.

2. Scope
This playbook applies to all employees, contractors, and third parties who use company email or communication platforms. It includes phishing attempts delivered through email, SMS, collaboration tools (Slack, Teams), and impersonation attacks.

3. Definitions
- Phishing: A fraudulent attempt to obtain sensitive information by disguising as a trusted entity.
- Spear Phishing: Targeted phishing directed at specific individuals.
- Business Email Compromise (BEC): Unauthorized use or impersonation of a business email account to commit fraud.

4. Roles & Responsibilities
End User: Report suspected phishing emails immediately.
IT Support: Quarantine emails, block senders, reset credentials.
Security Team: Lead investigation, determine scope, collect evidence, report findings.
Management: Approve communications and coordinate business impact discussions.

5. Incident Response Process
5.1 Identification
- User reports suspicious email to security team.
- SOC or IT validates indicators of phishing (sender, URLs, attachments).
- Determine if credentials were entered or links clicked.

5.2 Containment
- Quarantine email in mailbox and mail gateway.
- Block sender domain and associated IP addresses.
- If user clicked link: disable account temporarily.
- If device is compromised: isolate device from network.

5.3 Eradication
- Remove malicious emails across all user mailboxes.
- Delete unauthorized rules, forwarding filters, or inbox manipulation.
- Scan affected devices using EDR/AV tools.
- Revoke session tokens and reset credentials.

5.4 Recovery
- Restore normal account functionality.
- Monitor for reoccurrence or lateral movement.
- Notify impacted teams if confidential information was exposed.
- Reinforce training for targeted user(s).

5.5 Lessons Learned
- Conduct a post-incident review.
- Update security awareness training based on patterns.
- Modify email filters and detection logic as needed.
- Document findings and upload to incident tracking system.

6. Communication
Internal notifications may include:
- Impact summary
- Actions taken
- Required user follow-up (password reset, awareness reminders)

All external communications (customers, regulators, law enforcement) require approval from Legal and Executive Management.

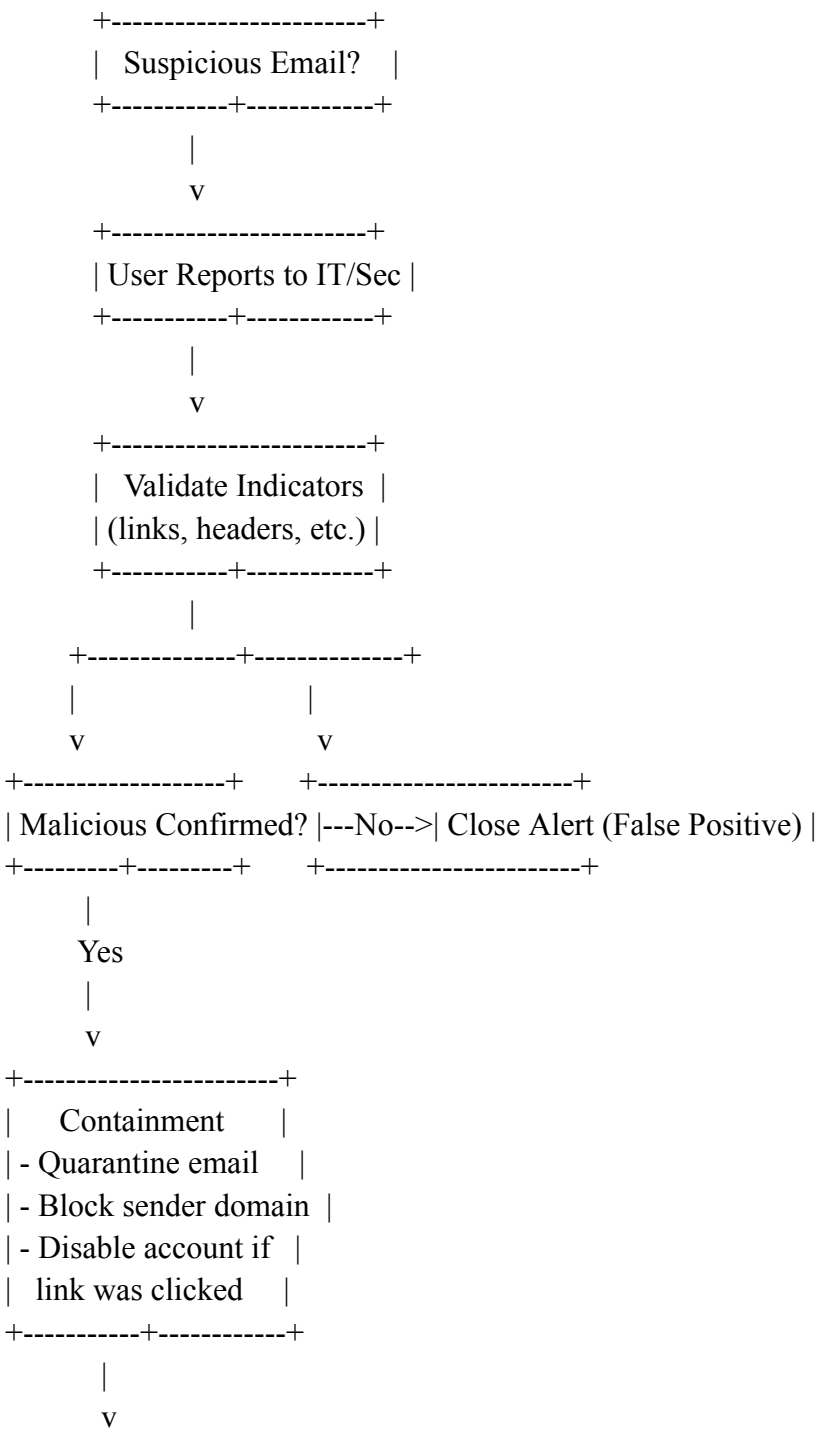
7. Evidence Handling
- Save phishing email headers, payloads, and timestamps.
- Export logs from email gateway, VPN, MFA provider, and device telemetry.
- Store evidence in designated incident repository following chain-of-custody rules.

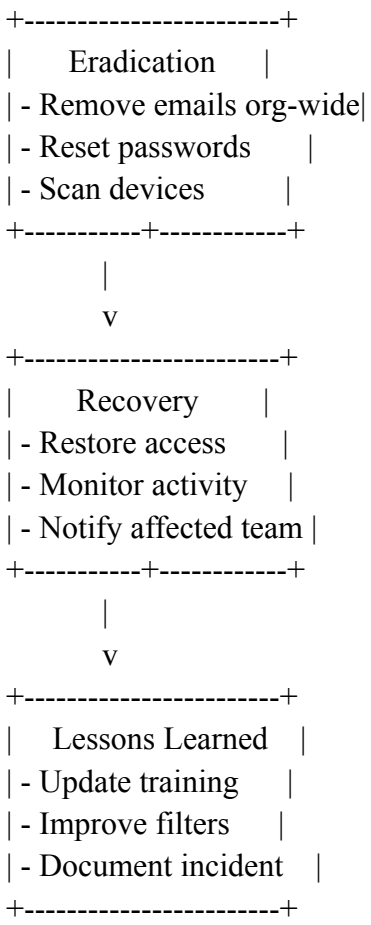
8. Metrics
- Time to detect
- Time to contain
- Number of users targeted
- Percentage of users who reported the email
- Recurrence rate

9. Violations

Failure to report suspicious emails or comply with response instructions may result in disciplinary action, up to and including termination.

10. Acknowledgment
All employees must comply with this playbook and complete phishing training annually.




Eradication
- Remove emails org-wide
- Reset passwords
- Scan devices
Recovery
- Restore access
- Monitor activity
- Notify affected team
Lessons Learned
- Update training
- Improve filters
- Document incident

Phishing Incident Response Checklist

Identification
[ ] User reported suspicious email
[ ] Indicators analyzed (headers, links, sender domain)
[ ] User asked whether links were clicked or credentials entered

Containment
[ ] Quarantined email in all affected mailboxes
[ ] Blocked sender domain
[ ] Disabled compromised accounts
[ ] Isolated affected devices

Eradication
[ ] Removed malicious emails across the organization
[ ] Reviewed inbox rules, forwarding, filters
[ ] Reset user passwords & revoked tokens
[ ] Performed full device scans

Recovery
[ ] Restored account access
[ ] Monitored login attempts
[ ] Verified no lateral movement occurred
[ ] Provided user guidance/training

Lessons Learned
[ ] Logged incident in tracking system
[ ] Updated security awareness material
[ ] Adjusted email filters and detection rules
[ ] Conducted post-incident review