Phishing incident playbook

Edition 16 November 2026. Free to copy and adapt under CC BY 4.0. Fields in [square brackets] are for you to fill in.

When to use this playbook

Use this playbook when staff report a suspicious message, or when a user clicked a link, opened a file or entered credentials after a message arrived by email, text or chat.

Before you start: prerequisites

Complete these before an incident, as part of planning.

- Mailbox auditing is on for all mailboxes, and message trace logs can be searched.
- Sign-in logs and endpoint alerts are kept and searchable.
- At least one identifier (email address or username) is known for each suspected target.
- Staff know how to report a message with one click or one phone call, and know they will not be blamed.
- Responders have the accounts and roles needed to search mail, reset sessions and remove messages.

Workflow

Work in this order. Record each step and its time in the incident log.

1. Identify and confirm the phishing message: get the original message and its message identifier.
2. Scope: find every recipient and whether each message was delivered.
3. Assess interaction: who opened, clicked or replied, and who entered credentials or ran a file.
4. Look for follow-on activity: new sign-ins, mailbox rules, forwarding, file downloads, new devices, lateral movement.
5. Contain: remove the message from all mailboxes; block the sender, link and domain; revoke sessions and reset passwords for exposed accounts; isolate any device that ran a file.
6. Prevent recurrence: add detections, adjust filters, and send a short note to staff.

Decision points

Stop at each of these and record the decision, the decider and the time.

Decision	Who decides	Information needed
Is any account or device compromised?	Technical lead	Sign-in logs, endpoint alerts, user interview
Is data exposed?	Technical lead, privacy lead	Mailbox access logs, downloads, forwarding rules
Is this one message or a campaign?	Incident lead	Recipient count, similar messages elsewhere
Is a payment request involved?	Incident lead	If yes, also open the business email compromise playbook

Notices to check

Open section 10 of the plan and confirm whether any of these start a notice clock.

- If personal data was accessed, start the data breach plan and the clocks in section 10.
- Report phishing to the national service for your country; CISA asks organizations to report to report@cisa.gov or its 24/7 line, and the FBI IC3 takes complaints.

Exit criteria and follow-up

Close the playbook only when all of these are true.

- No malicious messages remain in any mailbox.
- Every exposed account is reset and its sessions are revoked.
- No new suspicious activity for [period].
- Detections and filters are updated, and staff are told the outcome.