INCIDENT RESPONSE · RUNBOOK 04

Phishing response checklist

What to do in the first minutes after somebody reports, or admits, that they clicked.

DOCUMENT	VERSION	REVIEW CYCLE
IR-RB-04	1.0	Annual, and after every Sev 1 or Sev 2
OWNER	**APPROVER**	**CLASSIFICATION**
IT Manager (security operations)	Head of IT	Public reference copy

CONTROLS ADDRESSED

SOC 2 CC7.3, CC7.4, CC7.5 · ISO/IEC 27001:2022 A.5.24, A.5.25, A.5.26 · NIST SP 800-61r3 · NIST SP 800-53 IR-4, IR-6

Stance

Training reduces the rate. It will not reach zero, and an organisation that plans for zero improvises when it matters most.

Two rules make the rest of this work:

- **Contain before you investigate.** The instinct to establish severity first is understandable and wrong. Revoking access to somebody who turns out to be fine costs an apology. Waiting while it is assessed costs whatever the attacker does in that window.
- **Reporting must be free of blame.** A person who fears the response will not report, and a late report is far more expensive than a click. Whoever reports promptly has done the right thing and should be told so.

Severity

Classify within the first fifteen minutes on the evidence available, and revise as more is known. Classify upward when uncertain; downgrading later costs nothing.

LEVEL	DEFINITION	CONTAINMENT TARGET	ESCALATION
Sev 1	Privileged or administrative account compromised, or evidence of access to regulated, personal or customer data	Immediate, 15 minutes	Head of IT and leadership at once; legal and privacy owner engaged; incident bridge opened
Sev 2	Standard account credentials entered, multi-factor approved, or malicious software confirmed running on a device	30 minutes	Head of IT within 1 hour; legal and privacy owner on confirmation of data access
Sev 3	Link opened, no credentials entered, no software run, no session established	4 business hours	Handled in IT; summarised in the weekly report
Sev 4	Message received and reported, not interacted with	Next business day	Logged for trend analysis; no individual response required

A campaign reaching several people raises the level by one, because a targeted campaign implies preparation and often a second attempt.

Escalation and communication

Decide these before an incident rather than during one.

ROLE	RESPONSIBILITY
IT on call	Declares the incident, sets initial severity, performs containment
Head of IT	Accountable for the response; approves any downgrade of severity
Legal and privacy owner	Owns the notification decision at Sev 1 and Sev 2
Communications or leadership	Owns anything said outside the organisation
The affected person	A witness and a source, not a suspect

- **Sev 1 opens a bridge** and keeps a running timeline with timestamps.
- **A holding message goes to staff** where a campaign is widespread, saying what the message looks like and what to do. Speed matters more than polish.
- **Nothing goes outside the organisation** without the communications or leadership owner.

First ten minutes

1. **Revoke access.** Suspend the account. Do this before establishing how bad it is.
2. **Kill live sessions and tokens.** A suspended account can retain an active session. Revoke refresh tokens and application-specific passwords explicitly.
3. **Isolate the device.** Quarantine through device management rather than trusting the endpoint. Do not ask the user to run anything on it.
4. **Preserve evidence.** Keep the original message with full headers, and do not delete from the mailbox until it has been captured.
5. **Open a record** with a timeline. Every action from here carries a timestamp.

Establish what happened

- What was the message, and how did it reach the person? Note the sender, headers, authentication results and any spoofed display name.
- What did the user click, and what did the destination ask for?
- **Were credentials entered?** If so, treat them as compromised regardless of appearance.
- Was multi-factor prompted, and did the user approve it? Repeated prompts approved out of fatigue is a distinct and serious case.
- Was anything downloaded, and did it run? Check for installed software, browser extensions, and profiles added on the device.
- Were mail rules, forwarding addresses, delegates or recovery details changed? This is a frequent first move after a mailbox compromise and is easy to miss.
- Were any OAuth applications granted access to the account?

Establish the blast radius

- What could this account reach? Answer from role and group membership rather than memory.

- Did the same message go to anyone else? Search and remove across all mailboxes.
- Any sign-ins from unexpected locations, addresses or devices around the time of the click?
- Any access to shared data, and any unusual downloads or exports?
- Where the account held privileged access, treat every system it could reach as in scope until shown otherwise.

Recover

- Reset credentials and re-enrol multi-factor from a known-good path.
- Remove any mail rules, forwarding, delegates, extensions or application grants added by the attacker.
- Return the device to service **only once it is confirmed clean**, not once it appears fine and not because the user is waiting. Rebuild where there is any doubt.
- Restore access at the level the role calls for, rather than restoring what was there.

Close it properly

Limited exposure tempts everyone to close early. Run the full procedure anyway.

Severity is established at the end of an investigation, not at the start. A procedure only ever run on incidents someone correctly guessed were minor has not yet been tested.

Then answer three questions in writing:

1. **Why did the message arrive?** Filtering, authentication policy, or external sender marking.
2. **Why was the click possible or plausible?** Look at the pretext honestly. If it imitated a real internal process, the process is part of the problem.
3. **What limited the damage, and was that by design or by luck?** Design is repeatable. Luck is a finding.

Record what changed as a result. An incident that produces no change to a control, a policy or a piece of training has not been closed; it has only been survived.

Notification

Where regulated or personal data may have been reached, statutory notification obligations apply, and several carry hard deadlines measured in hours rather than days. The decision belongs to the legal and privacy owners, informed by what IT can establish about scope. IT does not make that call alone and does not make it in public.

Two practical points that decide whether the deadline is met:

- **The clock usually starts at awareness, not at confirmation.** Establishing scope quickly is part of meeting the obligation.
- **Record the basis for the decision either way.** A documented, reasoned conclusion that notification was not required is a defensible position. Silence is not.

Post-incident review

Every Sev 1 and Sev 2 gets a written review within 10 business days, and this document is reviewed after each one. The review covers the timeline, what worked, what did not, and the three questions above. Actions arising carry an owner and a date.