Phishing and account compromise response playbook

Playbook | English · Template to adapt | v3.0 · 2026-10-16

Template version: 3.0. For a smaller organization outsourcing IT or monitoring, the internal owner decides business risk while technical providers perform authorized actions within their actual access. People may combine functions with named deputies. Confirm supplier availability, support and recovery capabilities before adopting the procedure; do not assume a complete internal response team.

How to use this playbook. Sections 1–6 give the short sequence. Use responsibilities and branches in sections 7–8 during triage, then application, session and release checks in sections 10–12 before those measures. Activate section 9 whenever payment is involved; section 13 provides the example. Detailed references precede their decisions: their position after the summary does not postpone preparation until closure.

Type: adaptable operational procedure. Use this document for a suspicious message, credentials entered on a false site, an unexpected MFA approval or disputed account activity. Receiving a message, clicking and confirmed compromise are different states; document what is actually established. Adapt this playbook to the identity, email and application services you operate.

Approval and scope

Field	Value to complete
Organization, reference, version	[TO COMPLETE: organization, reference, version]
Owner and approver	[TO COMPLETE: security, authorized management]
Approval and next review	[TO COMPLETE: dates]
Covered services and populations	[TO COMPLETE: email, applications, staff, suppliers]
Incident and coordination	[TO COMPLETE: reference, lead, deputy]
Reporting and independent contact	[TO COMPLETE: channel, verified number]

The SOC assesses and preserves references. Email and identity teams act within their domains. Application owners control application sessions and permissions. Business owners assess restrictions' impact. Support verifies identity before assisting recovery. The incident lead arbitrates measures; legal and communications teams handle applicable obligations and external messages. Confirm these assignments against supplier contracts and actual delegated authority.

1. Receive without increasing exposure

☐ Ask for time, account, endpoint and actions taken without blaming the reporter.

☐ Distinguish opening, clicking, downloading, execution, secret entry and MFA approval.

☐ Preserve the original message, headers and identifier through the designated channel.

☐ Do not forward suspicious attachments to an ordinary distribution list.

☐ Do not request passwords, cookies, tokens or MFA codes in tickets.

☐ Contact the user through a verified means separate from the suspect account.

Do not open links from an administration workstation. File or URL analysis follows [TO COMPLETE: procedure, environment, authority]. A public analysis service may disclose submitted content: check

sharing rules before uploading. If the user cannot recover the original message, record that limitation and obtain available server-side references rather than asking them to recreate the interaction.

2. Assess exposure

Observation	Proposed check	Measure requiring authorization
Message received; interaction unconfirmed	Distribution, recipients, detection rule	Targeted removal if maliciousness is confirmed
Credentials entered or MFA approved	Sign-ins, registered methods, sessions	Account restriction and controlled recovery
File executed	Endpoint state, processes, connections	Endpoint containment according to risk
Disputed application operation	Application logs, target, result	Application-side measure and preservation

These are triage directions, not automatic rules. Adapt urgency to account privileges, sensitive services and ongoing activity. Define escalation criteria in [TO COMPLETE: severity matrix]. An MFA-satisfied sign-in does not explain every later action. Record whether the investigation links an action to a specific session or only to the same account.

3. Preserve a useful timeline

Correlate authentication, renewals, security changes and application operations. Retain stable account identifiers, application, result, time zone, diagnostic identifiers and source evidence. Record missing or expired log categories. Do not attribute an operation to a specific sign-in without a reliable session link. An unexplained gap should prompt a coverage question, not an assumption that the account was inactive.

For email, examine unusual rules, forwarding, delegation, messages sent and deletions. Review recent MFA-method changes, application permissions and roles. Microsoft recommends relevant checks for compromised email accounts; apply them only to available services and authorized investigation scope. A legitimate delegation or forwarding rule can resemble suspicious activity, so seek a verifiable business explanation before concluding that a change was hostile.

For payment fraud, activate the internal finance process and verified banking contacts promptly. Do not reuse contact details supplied in the suspicious message. Record confirmed amounts and transactions in the designated restricted space without unnecessarily spreading personal information. Operational urgency and the evidence needed for financial decisions should be coordinated with the responsible team.

4. Regain control and verify

☐ Authorize account restriction with awareness of business consequences.

☐ Reset compromised secrets through a trusted channel and endpoint.

☐ Revoke affected access at the identity provider and applications.

☐ Review and remove unauthorized methods, delegations or consents.

☐ Assess endpoint compromise before entrusting it with new secrets.

☐ Verify measures after execution, recording time and operator.

A password change does not demonstrate the end of every session. Microsoft documents differences between tokens and application cookies, and possible revocation delays. Have each service owner verify the result rather than treating a revocation button as universal proof of containment. Where a supplier performs the action, retain its confirmation and identify any verification that remains unavailable.

5. Reduce collective exposure

Search for related messages using several criteria: identifiers, technical sender, content, URLs and attachments. Check false positives before broad removal or blocking. Avoid blocking a legitimate shared service using one weakly specific indicator. Record measures' scope, duration, owner and rollback. Distinguish an indicator match from evidence that a recipient interacted or an account was compromised.

Inform exposed people with practical instructions: report interaction, reject unexpected prompts and use official channels. External notifications depend on the facts, contracts and applicable obligations; competent advisers determine recipients and deadlines. Use a consistent, approved message that does not disclose unnecessary incident details or expose investigation evidence.

6. Return to normal operation

☐ Confirm identity before reactivation or new MFA enrollment.

☐ Check expected rights, recovery and known unauthorized changes.

☐ Obtain functional validation from the user and application owner.

☐ Define targeted monitoring: [TO COMPLETE: period, events, owner].

☐ Record the conclusion, uncertainty and preventive actions.

☐ Test the process with an authorized fictional scenario and no real secrets.

Limitations: this playbook does not independently prove compromise, exfiltration or their absence. Privileged accounts, non-human identities and critical endpoints require additional procedures. Provider behavior and local authority remain decisive. Any unresolved verification must remain visible in the recovery decision.

Decision record and recovery check

Name an owner for every measure, including supplier actions. The record must go beyond “password changed”: state the access targeted, confirmed operations, measures completed and verification limits. If an application provides no usable confirmation, preserve that limitation and obtain acceptance of the residual risk from the authorized decision maker.

Proposed recovery element	Local value and evidence
Account and MFA-method control	[TO COMPLETE: check, operator, time]
Sessions and application permissions	[TO COMPLETE: applications, observed effect, unknowns]
Endpoint and recovery-channel check	[TO COMPLETE: tested scope, restrictions]
Reactivation and follow-up	[TO COMPLETE: decision maker, business acceptance, monitoring, end]

For a campaign affecting several people, distinguish exposed recipients, reported interactions and accounts with confirmed unauthorized actions. This supports proportionate measures without promising perfect attribution. During lessons learned, review reporting, recovery and missing checks; do not replace examination of protections with blame directed at the user.

7. Prepare people, scope and contacts

Map email, identity, SaaS, remote endpoints and supplier access. For each service, identify who can restrict accounts, export records and check sessions. An MSSP may detect without administering; the internal coordinator must know which provider can act. Keep missing permissions, licensing limits and coverage hours visible rather than assuming the monitoring supplier owns every response capability.

Decision	Proposed internal authority	Execution and confirmation
Restrict ordinary account	Coordinator within delegation	Identity administrator; targeted account/services checked
Block application or delegation	Business owner with security advice	Authorized administrator; scope/dependencies verified
Suspend payment	Authorized finance owner	Finance and verified bank contact; request reference
Reactivate or accept exception	Business owner or management	Provider; criteria met or residual risk accepted

The initial case records an internal reference, stable account, affected services and independent contact. If support is unavailable, use backup contacts and contractual escalation. Document attempts and consequences; propose available protection or business suspension. Do not claim a session was revoked merely because a ticket was opened. Name an internal person to follow each supplier request to its result.

For privileged or shared accounts, identify dependent activities before restriction. For supplier identities, contact the internal sponsor and contract owner. Safety-sensitive systems need an appropriate decision before disconnection. Urgency grants no authority to act on personal equipment outside approved scope. Record restrictions that technical responders cannot safely apply and the person deciding what happens next.

8. Choose a response branch and its evidence

Observed input	Proposed action	Decision and expected evidence
Message without established interaction	Preserve original; assess content/distribution	Justified targeted removal; message/scope retained
Credentials entered or unexpected MFA approval	Check account, sessions, methods, applications	Proportionate restriction; effect checked per service
Suspect download or execution	Assess endpoint and relevant connections	Risk-based isolation; state/limits recorded
Payment request or bank-detail change	Activate finance through known contacts	Suspension or independent verification; recorded decision

Branches can overlap. A message may lead to application consent without file execution; fraud may use a lookalike address without compromising your account. Record the observed route. If a person cannot recall their actions, preserve alternative hypotheses and seek supporting sources. Do not ask them to repeat a click or supply a secret to complete the form.

An account-compromise conclusion needs case evidence, not just a deceptive message. Conversely, recognition of a familiar sign-in does not necessarily explain a disputed application change. The coordinator may approve precautionary action under uncertainty while describing business impact, evidence needs and the reassessment condition. Keep temporary risk decisions distinct from a final finding.

9. Examine business email compromise and payment

Here, BEC means fraud using email or impersonation of a business context. Examine the original request, conversation, bank-detail changes, approvals and actual payment state. Preserve references in restricted storage. Neither invoice size alone nor a displayed sender address establishes fraud or human

complicity. Finance and technical responders must exchange the information needed for decisions without unnecessarily circulating banking or personal data.

Finance uses established bank contacts to request measures available for the transaction's actual state. Retain contact, time, reference and confirmed outcome. A recall request is not a recovery guarantee; obtain the appropriate result confirmation. Internal authorities determine external steps with competent advice under applicable obligations. This template sets no universal legal reporting deadline or guaranteed banking response.

Finance record to copy	Value to complete
Transaction and confirmed state	[TO COMPLETE: reference, amount, currency, checked state]
Business validation	[TO COMPLETE: approver, independent channel, evidence]
Bank request	[TO COMPLETE: known contact, time, reference, requested measure]
Result and follow-up	[TO COMPLETE: confirmation, uncertainty, owner, next decision]

Preserve necessary messages before bulk removal where urgency permits. Removing messages may prevent recipients accessing them, so coordinate evidence preservation with technical staff. If removal must come first, record lost evidence and remaining sources. Do not postpone urgent protection solely to complete a perfect investigation record; explain the tradeoff and authority instead.

10. Check applications, consent and email rules

For each suspect application, retain identifier, displayed publisher or owner, permissions, beneficiary and available events. Ask the business owner whether it is expected. A reassuring name does not establish authorization; an application unfamiliar to the analyst is not automatically malicious. Investigate permission scope and actual activity separately, preserving unknowns where logging does not support the conclusion.

Microsoft Entra documentation distinguishes administrator-consented permissions from user-consented permissions; revocation may require different interfaces. The executor must identify the grant type and follow the official procedure appropriate to their permissions. This template does not prescribe bulk deletion commands. Check equivalent provider-specific mechanisms for other platforms rather than assuming Entra behavior applies everywhere.

Object	Proposed check	Expected output
Consent or application access	Scope, beneficiary, history, business need	Justified retention or authorized removal with effect/limits
Email rule	Conditions, destination, activation, available creation history	Preserved original; decision and final state checked
Delegation or role	Beneficiary, rights, sponsor	Approval found or proportionate restriction
Recovery or MFA method	Addition, holder, independent validation	Expected method confirmed or controlled recovery

Do not limit checks to rules visible in an email client. Microsoft's compromised-account guidance includes administrative checks of rules and forwarding. Available tools and provider permissions determine coverage. Ask what was examined, what remains outside scope and who must complete it. Preserve the answer so “rules checked” cannot later be mistaken for an exhaustive review.

11. Session containment: distinguish request from result

Maintain separate entries for passwords, authenticators, tokens, application sessions, permissions and endpoint state. Record the authorized action, executor and available evidence for each. Microsoft documents that application-issued cookies depend on the application; do not infer their termination from password reset or an identity-side action alone. Missing confirmation remains an open limitation.

Measure and target	Executor	Verification and failure
Identity restriction	[TO COMPLETE: administrator/provider]	Suitable check; if unproven, retain protection/escalate
Application session	[TO COMPLETE: service owner]	Provider-specific effect; unknowns stated
Consent or delegation	[TO COMPLETE: authorized administrator]	Before/after state and dependencies; authorized rollback if mistaken
Suspect endpoint	[TO COMPLETE: endpoint operator]	Scope assessed; no new secrets without a decision

Reactivation requires a controlled recovery channel, verified expected rights, treatment of identified unauthorized changes and assigned monitoring. If a service cannot verify its sessions, the authority may defer recovery or accept documented compensating protection. No new alert is not a substitute for checking the intended effect. State which services are ready and which remain restricted.

12. False positives, exceptions and release

A restriction may affect legitimate activity. Before release, recover the initial rationale, obtain independent confirmation of need and verify that the targeted risk is treated or accepted. The same owner approves release or explicitly appoints a replacement. Retain evidence, scope, time and result; do not erase case history to simplify the record.

Exception or release record	Value to complete
Scope and business need	[TO COMPLETE: account, service, essential operation]
Risk and compensation	[TO COMPLETE: threat, verified restriction, limit]
Authority and decision	[TO COMPLETE: name, rationale, date]
End and check	[TO COMPLETE: expiry, monitoring, trigger, owner]

13. Complete example — entirely fictional

Workshop-80 receives a false bank-detail-change request in an order conversation. At 10:10 UTC, a finance employee reports opening a page and consenting to an application they believed necessary. The coordinator opens EX-P1 and verifies identity through a known internal number. IT administers email; the MSSP receives selected alerts only. All following times and results are fictional.

Fictional observation	Evidence	Supported conclusion	Action and owner
Bank-detail change request	EX-P-E1, original message	Request received; legitimacy unproven	Finance verifies supplier through known contact
Application grant found	EX-P-E2, administrative export	Permission present; actual use needs examination	IT determines scope and removes after authorization

Fictional observation	Evidence	Supported conclusion	Action and owner
Disputed forwarding rule	EX-P-E3, export/state	Change confirmed; human actor not attributed	Email owner preserves and checks
Payment still awaiting approval	EX-P-E4, finance confirmation	Business state confirmed at that time	Finance suspends within delegation; bank contact if needed

The fictional password reset is confirmed, but application sessions are not marked closed. IT examines service mechanisms and retains uncertainty about an external application. Management approves partial recovery without that application, with ownership and reassessment. A legitimate business rule found during the search remains in place: the team does not indiscriminately remove every forwarder.

Accept the exercise if a replacement can distinguish receipt, interaction and activity evidence, locate finance decisions and identify access still needing checks. Fail it if successful MFA closes the case, a revocation request counts as universal proof or business needs are never considered. Assign a corrective action and result check to each gap before accepting readiness.

Working references

For application permissions, also consult Microsoft: reviewing and revoking application permissions. Check current interfaces and required permissions before acting.

Microsoft: compromised email account response; Microsoft: access revocation; NIST SP 800-61 revision 3. These references support the framework. The sequences and checks are proposals to adapt, without a compliance guarantee.