OpsAtlas™
OPERATIONAL RUNBOOKS BY SMALLWOOD ENTERPRISES
Reliable cloud operations documentation

Reported Phishing Email Triage

Cybersecurity Incident Response Runbook 01

Cybersecurity Incident Response Runbooks

2026-05-30

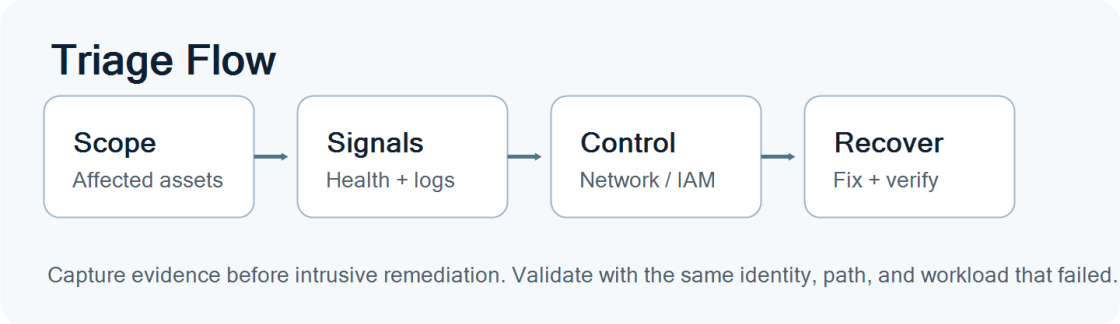
Table of Contents

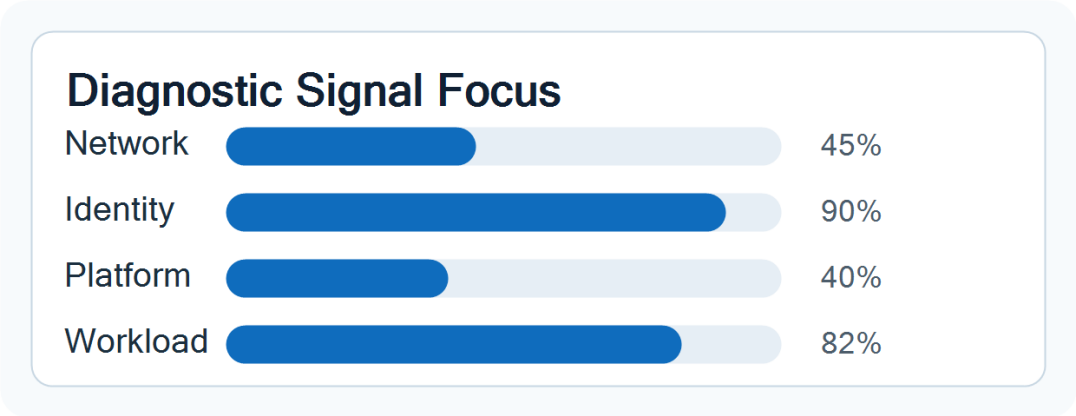
Reported Phishing Email Triage

Cybersecurity Incident Response Runbook 01
Audience: security analysts, service desk escalation teams, MSPs, Microsoft 365 administrators, endpoint administrators, and IT operations leads
Severity guide: Sev 1 when ransomware, active compromise, data exfiltration, privileged access abuse, widespread malware, or business-critical identity impact is suspected; Sev 2 when a contained user, endpoint, mailbox, application, or policy issue requires urgent triage.
Incident objective: Determine whether a reported email is malicious, benign, or suspicious; preserve evidence; remove related messages; and guide affected users.

> **Operator note:** Capture who is affected, when it started, exact error text, device/service identifiers, request IDs, screenshots, and before/after evidence.

Prefer the smallest reversible change that restores service, then replace emergency access with a durable fix.





Common Symptoms

- User reports a suspicious email, link, QR code, attachment, invoice, voicemail, or shared document.
- Multiple users report similar sender, subject, attachment, or URL.
- A user clicked a link, opened an attachment, or entered credentials.

First 15 Minutes

- Preserve the original message, headers, sender, recipients, subject, URLs, attachment hashes, and received time.
- Check Defender, mail trace, quarantine, and user report submissions.
- Search for related messages by sender, subject, URL, attachment name, and message ID.
- Determine whether any user clicked, replied, downloaded, authenticated, or approved MFA.
- Escalate immediately if credentials, payment instructions, or malware execution are involved.

Command Starters

Replace placeholders before running. Use the approved admin context and record output in the ticket.

```
Get-MessageTrace -SenderAddress <sender> -StartDate <start> -EndDate <end>

Get-MessageTraceDetail -MessageTraceId <id> -RecipientAddress <recipient>

Search-UnifiedAuditLog -StartDate <date> -EndDate <date> -UserIds <user>

Get-QuarantineMessage -SenderAddress <sender>
```

Decision Path

If you find...	Do this next
Message is confirmed malicious	Purge related messages, block indicators, and start user-impact review.
User clicked or entered credentials	Reset password, revoke sessions, review MFA/device state, and inspect mailbox activity.
False positive	Release or allow narrowly and submit to improve filtering.
Business email compromise indicators exist	Escalate to mailbox compromise and payment-fraud workflow.

Remediation Actions

- Submit the message to the security platform or Microsoft for analysis.
- Purge confirmed malicious messages from affected mailboxes.
- Block sender, domain, URL, attachment hash, or infrastructure only as narrowly as possible.
- Notify affected users with clear next steps and avoid sharing live malicious links.
- Open related incident tasks for credential reset, mailbox review, and endpoint scan when user interaction occurred.

Validation Checklist

- Related messages are removed or contained.
- Indicators are blocked or monitored.
- User interaction is documented and remediated.
- Ticket includes original message evidence, search scope, and final disposition.

Evidence to Attach

- User, device, service, tenant, location, IP/network, timestamps, and exact error text.

- Screenshots, logs, health/status evidence, message traces, policy results, or admin-center audit entries.
- Before/after configuration for identity, licensing, endpoint, network, mailbox, policy, or device changes.
- Approval record for any emergency permission, data restore, policy bypass, account unlock, deletion, rollback, or public exposure.

Customer-Facing Summary Template

What happened: `<brief customer-safe description>`
Impact: `<users/services/locations affected and time range>`
Root cause: `<confirmed root cause or current leading cause>`
Resolution: `<fix applied and validation completed>`
Prevention: `<monitoring, guardrail, training, policy, or knowledge-base follow-up>`

Reference Anchors

- Microsoft Defender for Office 365
- Microsoft Defender XDR documentation
- NIST incident handling guide