ENTERPRISE RESOURCES

# Google Workspace Phishing Response Checklist

A phishing email can lead to credential theft, unauthorized account access, malicious OAuth application approvals, and exposure of sensitive business data.

This checklist provides a structured process for Google Admins responding to a suspected phishing incident. Follow the phases in order, starting with containment before moving into investigation, remediation, and prevention.

GAT labs

# Google Workspace
# Phishing Response Checklist

## Phase 1: Contain the Threat

- [ ] Confirm whether the user clicked a link, scanned a QR code, entered credentials, downloaded an attachment, or approved an application.
- [ ] Force sign out the affected user.
- [ ] Reset the user's password.
- [ ] Revoke connected third-party applications if compromise is suspected.
- [ ] Remove application-specific passwords and backup codes.
- [ ] Temporarily suspend the account if active compromise is suspected.

**KNOWLEDGE BASE ARTICLES**

Investigate Google Workspace Account Compromise with GAT+

## Phase 2: Identify and Remove the Phishing Email

- [ ] Before continuing the investigation, determine whether additional users received the same message.
- [ ] Identify the sender, subject line, and delivery timeframe.
- [ ] Determine which users received the email.
- [ ] Determine whether any users opened, replied to, or interacted with the message.
- [ ] Remove malicious emails from affected inboxes.
- [ ] Confirm the email can no longer be accessed by users.

**KNOWLEDGE BASE ARTICLES**

Delete Phishing Emails with GAT+

# Google Workspace
# Phishing Response Checklist

## Phase 3: Investigate What Happened Next

The phishing email is often only the beginning of the incident.

- [ ] Review login activity for unusual locations, devices, and sign-in attempts.
- [ ] Review Gmail forwarding rules and mailbox delegations.
- [ ] Review Google Drive activity for downloads, external shares, and sensitive file access.
- [ ] Review newly approved third-party applications.
- [ ] Review browser activity if available.
- [ ] Review account's access permissions and privileges.
- [ ] Build a timeline showing what actions occurred after the phishing email was received.

**KNOWLEDGE BASE ARTICLES**

How to Set Up User Security Alerts with GAT+

# Google Workspace
# Phishing Response Checklist

## Phase 4: Assess Potential Data Exposure

Determine what information may have been accessed, downloaded, or shared.

- [ ] Identify sensitive emails that may have been exposed.
- [ ] Review attachments sent externally during the investigation window.
- [ ] Identify files accessed or downloaded from Google Drive.
- [ ] Review newly created external shares.
- [ ] Identify external collaborators added during the compromise window.
- [ ] Determine whether regulated, financial, HR, or customer data may have been affected.
- [ ] Document findings for management, security, compliance, or legal teams.

**KNOWLEDGE BASE ARTICLES**

Monitor External Email Attachments with GAT Activity Report

Find and Take Action on All Shared-Out Files and Folders in a Domain

Remove External Collaborators from Google Drive

# Google Workspace
# Phishing Response Checklist

## Phase 5: Remediate and Recover

- [ ] Remove unauthorized forwarding rules.
- [ ] Remove mailbox delegations that should not exist.
- [ ] Revoke suspicious OAuth applications.
- [ ] Remove unauthorized external sharing permissions.
- [ ] Review group memberships and privileged roles.
- [ ] Confirm MFA remains enabled.
- [ ] Update account recovery settings if required.
- [ ] Notify affected users and stakeholders.

## Phase 6: Reduce Future Risk

- [ ] Review phishing protection settings in Google Workspace.
- [ ] Review third-party application policies.
- [ ] Configure alerts for suspicious email activity.
- [ ] Configure alerts for unusual login behavior.
- [ ] Review external sharing controls.
- [ ] Conduct periodic phishing simulation exercises to test user awareness and identify training gaps.
- [ ] Update phishing response procedures based on lessons learned.
- [ ] Schedule periodic phishing investigation exercises for administrators.

# Incident Summary

Use this section to document the outcome of the investigation.

Date of incident:

Affected user(s):

Root cause identified:

Account compromised: Yes / No

OAuth application involved: Yes / No

Sensitive data exposed: Yes / No

Remediation completed: Yes / No

Additional follow-up required:

# Want To Learn More?

VISIT OUR WEBSITE

VISIT OUR RESOURCES PAGE

TRAINING SESSIONS CALENDAR