

Google Workspace Phishing Remediation

Prepared by the Ottawa Area Cybersecurity Operations Center | Last updated 09/04/2026

Purpose

This guide provides an evidence-driven workflow for investigating and remediating phishing emails in Google Workspace. It helps teams determine scope, identify user interaction, remove malicious messages, preserve evidence, complete follow-up actions, and improve future detection and response.

Detection

- ☐ Confirm the email in question is not a false positive
 - ☐ Make note of whether or not the sender is a legitimate address that has been compromised
- ☐ Document findings

Determine Scope

- ☐ Determine what the malicious email is attempting to exploit (eg. malicious link leading to phishing portal, executable attachment, callback phishing attempt, etc...)
- ☐ Search **Gmail log events** in the Google Admin Console for the malicious email
 - ☐ How many internal recipients are there?
 - ☐ Did any recipients interact with the malicious link or attachment?
 - ☐ Did anyone respond to the malicious email?
- ☐ Check **User log events** in the Google Admin Console for anyone who interacted with a malicious link or attachment
 - ☐ Are there failed suspicious sign-in attempts?
 - ☐ Are there successful suspicious sign-ins?
- ☐ Check for **evasive delivery methods**
 - ☐ For Calendar event notifications, check **Calendar log events** in the Google Admin Console to collect eventIDs and attendee lists. In some cases, users' calendars may be set to automatically add invitations to their calendar. [See Google's documentation on this setting here.](#)
 - ☐ For legitimate Google Drive Share notification emails that lead to a malicious file, internal Drive logs **do not** show internal users accessing the file, since the owner is external. There is a feature request submitted to Google to reconcile this blind spot (upvote or comment please!): [Remove Google Drive file shared with users as a viewer](#)
 - ☐ **To check for users who accessed the file:**
 - Access **Google Vault** and search for the file's title, access the file to get the fileID. For example: `https://docs.google.com/document/d/[fileID]/edit?tab=t.0`
 - Look for "viewedByMe: **True**" and "viewedByMeTime" toward the bottom of results: `gam user [user email] info drivefile [fileID]`
- ☐ If the payload is an executable file and Gmail logs show a user interacted, check **device logs** in your environment to see if the malicious executable ran on the device
 - ☐ In cases where a device is suspected to be compromised, **Access Evaluation Logs** in the Google Admin Console can give more context on session cookies being stolen (filter by IP address)

Disable the Threat

- ☐ **Collect a copy** of the malicious email
 - `gam user [email] export messages query "in:anywhere rfc822msgid:<[messageID]>" targetfolder C:\Path\To\Destination.eml`
- ☐ **Remove the malicious email** from all user inboxes
 - `gam user [email] delete messages query "in:anywhere rfc822msgid:<[messageID]>" doit`
- ☐ **Collect evidence** of calendar invitations
 - `gam calendar [user email] print events query "[Event title]" todrive`

- ☐ **Remove the malicious invite** from all user calendars
 - gam user [compromised email] delete events primary event eventid [eventID] doit
OR
 - gam user [compromised email] delete event query “[Event title]” doit
- ☐ For legitimate Google Drive shares where the file being shared is malicious:
 - ☐ **Send an email to affected users** to notify them that the file is malicious, instruct them to remove the file from their “Shared with me” section of their Drive (if desired)
- ☐ If malicious sign-in attempts were observed, use the [Google Workspace User Compromise Remediation workflow](#)

Audit Logs & Clean Up

- ☐ If the sender is legitimate, **contact their organization** by phone and/or email to notify them of the compromised account in their environment
 - ☐ If the organization was not aware or did not answer, **add the sender to a temporary (7 day) compliance rule** to route incoming emails to the quarantine
- ☐ If the sender is not legitimate, **add the address to a permanent compliance rule** to route incoming emails to the quarantine (for visibility purposes)
- ☐ **Submit a site takedown request** for any malicious content being hosted by legitimate providers
 - ☐ Submit a report to [Google Safe Browsing](#) for the phishing portal
 - Consult the [Site Takedown Resources](#) document for more information (live document)

Learn Something

- ☐ **Consider the rules in place** that allowed the malicious email to be delivered
- ☐ **Assess if improvements can be made** to improve detection or prevention in the future
 - ☐ Quarantine rules, custom alerts, user processes, Admin Console settings, communication and/or training for recipients