

Google Workspace User Compromise Remediation

Prepared by the Ottawa Area Cybersecurity Operations Center | Last updated on 09/03/2026

Purpose

This guide provides an evidence-driven workflow for responding to suspected or confirmed Google Workspace account compromises. It helps teams contain access, review attacker activity, remove persistence, clean up malicious changes, document findings, restore user access, and identify security improvements.

Detection

- ☐ **Confirm the suspicious sign-in** on the user's account is not legitimate access
- ☐ **Document findings**

Determine Scope

- ☐ Review **User log events** to determine if the attacker established persistent access with 2SV or a passkey

Disable the Threat

- ☐ For accounts protected with 2-Step Verification, **revoke active sessions**
- ☐ For accounts not protected with 2-Step Verification, **suspend the account**
- ☐ **Remove 2SV methods or passkeys** added by the attacker, if present

Audit Logs & Clean Up

Review each of the following logs for activity from the malicious IP address(es) and remediate as necessary.

User log events

- ☐ Remove **forwarding rules** added by the attacker
 - gam user [email] show forwards
 - gam user [email] delete forward [forwardID]
- ☐ Remove **filtering rules** added by the attacker
 - gam user [email] show filters
 - gam user [email] delete filter [filterID]
- ☐ Remove **delegated access** added by the attacker
 - gam user [email] show delegates
 - gam user [email] delete filter [filterID]
- ☐ Remove **blocked addresses** added by the attacker
 - Must be resolved from within the user's interface: <https://mail.google.com/mail/u/0/#settings/filters>

Drive log events

Docs, Sheets, Forms, Drive

- ☐ **Save evidence** of content created by the attacker
 - gam user [email] get drivefile [fileID]
 - ☐ **Remove malicious content** created by the attacker from the compromised user's account
 - Recoverable (optional): gam user [email] delete drivefile [fileID]
 - Not recoverable: gam user [email] purge drivefile [fileID]
- Note:** Drive files shared from external accounts to internal users as a "viewer" [cannot be removed](#).
- ☐ If searches were conducted or items were viewed from malicious IP(s) see [Takeout log events*](#) (below) for further action steps

Scripts or Sites

- ☐ **Take ownership** of the malicious script or site
 - gam user [compromisedEmail] add drivefileacl [fileID] user [yourEmail] role owner
- ☐ **Access the file** from your UI
 - Scripts: [https://script.google.com/u/0/home/projects/\[fileID\]/edit](https://script.google.com/u/0/home/projects/[fileID]/edit) (replace [fileID])
 - Sites: [https://sites.google.com/d/\[fileID\]/p/\[file\(Home\)ID\]/edit](https://sites.google.com/d/[fileID]/p/[file(Home)ID]/edit) (replace [fileID] and [file(Home)ID])
- ☐ **Document your findings** by taking screenshots and/or copying the malicious script to a text file
- ☐ **Archive active script deployments**
 - Deploy > Manage Deployments > Archive (button in upper right of window)
- ☐ **Delete** the malicious Script or Site
 - gam user [email] purge drivefile [fileID]

Gmail log events

- ☐ Filter by “Owner is [compromised user]” to identify actions the attacker took in the user’s mailbox and **collect messageIDs**, including:
Emails drafted, emails sent, bounce notifications, responses to emails sent
- ☐ **Save evidence** of content created or any activity related to malicious actions taken
 - gam user [email] export messages query "in:anywhere rfc822msgid:<[messageID]>" targetfolder C:\Path\To\Destination.eml
- ☐ **Delete malicious (or related) content** in the compromised user’s mailbox and for all internal recipients
 - gam user [email] delete messages query "in:anywhere rfc822msgid:<[messageID]>" doit
- ☐ **Email external recipients** of malicious emails sent by the attacker from the compromised account
- ☐ If “View” or “Open” events are observed from malicious IP(s), **see [Takeout log events*](#)** (below) for further action steps

OAuth log events

- ☐ **Check for access granted** during the period of compromise or by known malicious IP addresses
 - ☐ Review activity to distinguish between legitimate and illegitimate use
- ☐ **Display tokens** to get the clientID(s) and view associated scopes
 - gam user [email] show tokens
- ☐ **Document findings** by taking screenshots or copying tokens to a text file
- ☐ **Investigate scopes and app activity** to determine what the apps were being used for and if any further remediation is necessary
- ☐ **Revoke access** where applicable
 - gam user [email] delete token [clientID]

Calendar log events

- ☐ Filter by “Owner is [compromised user]” to identify actions the attacker took in the user’s calendar and **collect eventIDs**.
- ☐ **Save evidence** of events created or distributed from the compromised account
 - gam calendar [compromised email] print events query “[Event title]” todrive
- ☐ **Delete malicious content** in the compromised user’s calendar and for all internal attendees
 - gam user [compromised email] delete events primary event eventid [eventID] doit
OR
 - gam user [compromised email] delete event query “[Event title]” doit

- ☐ Repeat [Gmail log events](#) steps for **emailed calendar notifications** sent to internal users

Chat log events

- ☐ **Collect spaceIDs** for chat messages created by the attacker (filter by malicious IP(s))
- ☐ **Display messages** to collect message Name(s)
 - gam user [email] show chatmessages space [spaceID]
- ☐ **Document findings** by taking screenshots or copying results to a text file
- ☐ **Delete messages**
 - gam user [email] delete chatmessages name [messageName]

Takeout log events*

*Action steps listed here are optional based on findings, district comfort level, responsible disclosure, etc.

- ☐ **Review & classify** data accessed or exported by the attacker
- ☐ **Seek guidance** from your cyber insurance provider
- ☐ **Prepare disclosures** for affected parties
- ☐ **Seek legal review of disclosures** before distribution

Learn Something

- ☐ Consider the rules in place that allowed the sign-in to be successful
- ☐ 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 affected parties
- ☐ Deliberate on any security measures that can be implemented to mitigate the impact of a compromise in the future