Global Digital Forensics · Guide edition 2026-11-03 · evestigate.com/insights/stolen-access-token-evidence/

EMAIL AND CLOUD EVIDENCE

Preserving Microsoft 365 and Google Workspace Evidence After Token Theft

A stolen session token keeps an intruder inside an executive mailbox after the password is reset, while the sign in and audit records the examiner reads to see what was taken run on a rolling retention schedule. Export the identity and mailbox logs as you contain the account, and call (800) 868-8189 at any hour.

Published September 19, 2026 · Updated October 30, 2026

Request a Confidential Consultation on a compromised business account

If suspicious account activity affects your business, identify the service, the event and when an answer is needed.

Discuss a compromised business account

Discuss the available records and a secure way to share them.

Business email compromise analysis

Account activity, suspicious messages and changed payment instructions.

Microsoft 365 and email evidence

Preserve and examine the messages and related activity records.

By Joseph Caruso, Founder, CEO and CTO, Global Digital Forensics

© 2026 Global Digital Forensics, Inc. All rights reserved.

Why Token Theft Calls for More Than a Password Reset

When an adversary compromises a corporate Microsoft 365 or Google Workspace account today, they rarely rely on simple password guessing alone. Modern threat actors deploy adversary in the middle phishing proxies and infostealer malware to capture authenticated browser session cookies and OAuth access tokens after the legitimate user completes multi factor authentication. Once that session token is stolen, the intruder can replay it from their own infrastructure to access executive mailboxes, SharePoint repositories and Google Drive folders without triggering another multi factor prompt.

A complete response pairs the password reset with revoking active session tokens and rogue enterprise OAuth applications, which frequently stay valid through a reset, and with exporting the cloud audit trail while it is within its rolling retention window. Global Digital Forensics performs rapid cloud forensic analysis and telemetry examination engagements directly for retained attorneys, internal auditors and corporate IT security teams who lead the response.

Which Volatile Identity and Mailbox Records to Preserve First

Defending your organization before regulators, cyber insurers or the other side in litigation starts with a documented account of how the account was accessed and which specific records were viewed or exfiltrated. Under the direction of your legal team or security leadership, our examiners prioritize the immediate export of the Microsoft Entra ID interactive and non interactive sign in logs, which Microsoft keeps for seven or thirty days depending on licence, together with the Microsoft Purview Unified Audit Log and the Google Workspace Admin audit logs, which run on longer published retention windows. We correlate session identifiers, IP address shifts, user agent strings and MailItemsAccessed events to distinguish automated background synchronization from deliberate human browsing inside an executive mailbox.

What the Identity Record Shows and How It Is Read

Two questions usually come first: how did the intruder get in, and what did they see. The identity record speaks most directly to the first, and the second calls for careful reading of the mailbox audit record. Microsoft Entra ID sign in logs record the session identifier, the token issuer, the device identifier when one is registered, the client application, the IP address and the user agent for each interactive and non interactive sign in. When a session identifier created on a managed laptop in the finance office reappears minutes later from a hosting provider address with a different user agent and no new multi factor prompt, that pattern is consistent with token replay rather than a password guess. We document the pattern, the time offsets and the token lifetime involved so the mechanism can be described with each entry stated at its true weight.

The second question takes more care, and we explain the method plainly. The MailItemsAccessed operation in the Unified Audit Log records when mail items were accessed through a bind or sync operation, and it aggregates events and throttles logging once a mailbox exceeds a threshold within a short window. This means a record can show that a set of folders was synchronized by a foreign session, and the examiner then reads the folder contents and any item level events to assess which messages that session opened. Google Workspace exposes similar access telemetry through its audit logs under its own recording rules. We separate the folders and date ranges that the log affirmatively shows from the ones we infer, because an insurer, a regulator or opposing counsel will press on the difference.

© 2026 Global Digital Forensics, Inc. All rights reserved.

Tying activity to a person combines the device record with access logs, interviews and other corroboration. An IP address points to infrastructure, and a residential proxy can route an attacker through any location, so our reports describe the actor as the session or the account, and attribution to a named individual rests with counsel and with law enforcement where their own investigation warrants it. That discipline protects the client, because a report that stays with the data gives every finding around it a firm footing under cross examination. Our compromised account analysis service describes the artifacts we rely on for this work.

Retention Clocks Published by Microsoft and Google

Preservation urgency in a token theft case comes straight from the retention schedules the providers publish. Microsoft states in its Entra data retention reference that sign in log data is kept for seven days on the free tier and thirty days with a Premium P1 or P2 license, and the examiner checks whether the tenant also routed it to a log analytics workspace, a storage account or a SIEM, which keep copies on their own schedule. The Unified Audit Log in Microsoft Purview keeps records for 180 days on the standard tier under the published audit retention policies, with longer retention where the organization licensed and configured it. Google publishes data retention and lag times for each Workspace audit log, and several of the most useful logs are retained for six months.

Those windows matter because the first days after a compromise are usually consumed by containment, insurance notice and internal fact finding, and the sign in records that explain the entry point run on the shortest clock. We export the Entra sign in logs, the audit log search results for the affected accounts, the OAuth consent grants, the inbox rule and transport rule configuration and the mailbox audit records in native JSON or CSV, hash each export and record who ran it, from which admin account, and when. The export itself becomes evidence of reasonable steps if preservation is later questioned under Federal Rule of Civil Procedure 37(e).

A claim against the intruder runs through the federal computer fraud statute, and a claim against a vendor whose account was the entry point draws on the same sign in record. Section 1030 reaches whoever “intentionally accesses a computer without authorization or exceeds authorized access” (18 U.S.C. 1030). The sign in and token records are where the examiner looks for evidence that an access occurred, that it came from someone other than the account holder, and when it happened, so preserving them early serves both the civil claim and any report to law enforcement. An export made in time preserves the record in the form courts expect.

How a Token Compromise Examination Runs and Protects You

The engagement begins with a scoping call in which we identify the affected identities, the tenant type and license tier, whether logs are already flowing to a SIEM, and whether anyone has reset passwords, revoked sessions or deleted rules. We ask before we act because every one of those actions changes the record. Preservation follows immediately, with exports hashed and logged. We then reconstruct the identity timeline: first anomalous sign in, token issuance, device registrations, multi factor method changes, consent grants to enterprise applications and any additions to privileged roles. This phase establishes how the intruder got in and whether the entry was phishing, infostealer malware on an endpoint or a third party application.

© 2026 Global Digital Forensics, Inc. All rights reserved.

The second phase reconstructs what the session did. We correlate MailItemsAccessed, SharePoint and OneDrive file access events, eDiscovery search activity, mail forwarding and the creation of inbox rules that hide replies, and we compare the session identifiers in each event to the compromised sessions identified in phase one. Where the data shows a sync of specific folders, we inventory those folders so counsel can assess exposure of privileged communications, personal data or deal information. This is the work that supports notification analysis and insurer reporting, and it rewards the time it takes.

The final phase is a persistence check and a written record. Stolen tokens are often paired with a second foothold: a registered authenticator on an attacker device, a rogue application with mail read permissions, a forwarding rule to an external address or a new guest account. We document each and confirm with the administrators that the removals occurred after preservation. The deliverable is a report that walks from the preserved exports to each finding, written for counsel and the security lead, and it can be converted into a declaration if the matter proceeds. The Microsoft 365 forensics and Google Workspace forensics pages describe the platforms this covers.

Reading the Findings From the Legal, Insurance and Security Seats

Anyone reading a token compromise report should look first at the boundary between what the log shows and what the examiner infers, because that boundary governs notification decisions and litigation exposure. A finding that a session synchronized the Inbox and Sent Items folders between two timestamps is a statement of record. A finding that the intruder read a particular contract rests on an item level access event where one exists and is otherwise labeled an inference. We mark the difference in the report, and we recommend that notification letters and insurer submissions use the same language. Our guide to the first 24 hours of a business email compromise covers the parallel finance and recall tracks.

A security lead reads the same report for control improvements. The questions are whether conditional access permitted a sign in from an unmanaged device, whether token lifetime and continuous access evaluation were configured, whether user consent to third party applications was open, and whether the SIEM captured records beyond the tenant's own retention. We write the control observations in a separate section from the factual timeline so the security team can act on them while the factual timeline stands on its own in later litigation. Our forensic readiness planning service helps organizations put those controls in place ahead of the next incident.

Internal auditors and insurance liaisons use the chain of exports and hashes to confirm that the analysis rests on preserved data rather than screenshots from an administrator console. Every export is listed with its hash, the account that produced it and the time it was produced, so a later reviewer can reproduce the analysis from the same files. That record is what lets the report move from an internal document to a declaration in support of a motion or a response to a regulator as it stands, and it is the first thing we assemble because it anchors everything that follows.

© 2026 Global Digital Forensics, Inc. All rights reserved.

Immediate Preparation Steps for Legal and IT Teams

Time is of the essence the moment unauthorized cloud access is suspected. Have your Global Administrator export the raw authentication logs and the mailbox forwarding rules in their native format first, and keep the account and its licence in place, because deleting an account or removing a licence starts Microsoft's purge clock on the user's data. Once the volatile telemetry is cryptographically hashed and preserved, your administrators can revoke active refresh tokens, purge rogue OAuth grants and enforce compliant conditional access policies.

You can inspect individual suspicious email messages right now using our zero upload Email Header Analyzer (evestigate.com/tools/email-header-analyzer/), read our guide to the first 24 hours of a business email compromise, or call Global Digital Forensics 24/7 at (800) 868-8189 to initiate an immediate cloud preservation engagement. The initial consultation is free.

Retention Clocks by Source and License

The guide explains why the identity record is the first thing to export. This table gathers the published retention windows for each source a compromised account examination relies on, together with the question each source answers and the moment it should be exported. Read the license column against your own tenant, because one enterprise often holds a Premium tenant at headquarters and a free tier tenant at an acquired unit. Where a cell says the record persists until removed, the export simply comes before the cleanup.

Published retention windows and preservation priority for the sources examined after a suspected account compromise.

Source	Published retention	What it answers	When to export
Entra sign in logs, free tier	Seven days per Microsoft	Whether a session appeared from new infrastructure without a new MFA prompt	Within hours of suspicion
Entra sign in logs, Premium P1 or P2	Thirty days per Microsoft	The same record with a longer window to find first entry	Within the first day
Purview Unified Audit Log, standard tier	180 days per Microsoft	MailItemsAccessed, file access, rule creation and consent grants	Before any account changes
Google Workspace audit logs	About six months for several logs per Google	Gmail, Drive and login events by session and address	Before any account changes
OAuth application consents	Persist until revoked	Standing mail or file access that survives a password reset	Inventory before revoking
Inbox and transport rules	Persist until deleted	Forwarding and reply suppression set by the intruder	Export conditions before deleting
SIEM or Log Analytics workspace	Set by the organization	Copies held beyond the tenant's own retention	Confirm coverage on the first call

© 2026 Global Digital Forensics, Inc. All rights reserved.

Trace the Suspicious Message in the Email Header Analyzer

If a suspicious message sits in the compromised mailbox, open the original in your mail client, copy the complete raw header block rather than the few lines the reading pane shows, and paste it into the Email Header Analyzer (evestigate.com/tools/email-header-analyzer/). It lays out every Received hop in order with its timestamp, shows whether SPF, DKIM and DMARC passed for the sending domain, and checks the DKIM body hash against the message body. A chain of hops that ends at an unfamiliar relay, or a DKIM pass for a domain other than yours, points to a message from outside even when the display name says otherwise. The analysis runs in your browser and the headers stay on your machine. When the headers raise a question about your own tenant, call, because the next step is in the sign in logs, which the examiner reads directly.

How to Begin and What Happens on the First Call

Our Business Email Compromise Checklist: Preserve Before You Clean Up sets out the items to secure in the order they expire. For the first call, gather the affected account names, the time the activity was noticed, who holds Global Administrator rights, the tenant license tier, whether logs are forwarded to a SIEM, and a list of any resets, revocations or rule deletions already made. On the call the examiner asks how the compromise was discovered, what has changed since, whether funds or data appear to have moved, and whether the legal team is directing the response. We then recommend immediate preservation steps for your administrators and send a written proposal that names the sources, the sequence, the deliverable and the timing drivers based on the tenant configuration you describe. The initial consultation is free. Call (800) 868-8189 at any hour, or request a scheduled conversation.

Technical References and Further Reading

Primary sources and provider documentation behind this guide: NIST's September 2026 announcement on protecting online identity and access tokens, Microsoft sign in documentation, Microsoft account compromise guidance, Microsoft retention documentation, September 2026 identity compromise analysis and mailbox auditing guidance.

Authorities cited in this guide: Microsoft Entra data retention reference. Establishes the seven day and thirty day retention of Entra sign in and audit logs by license tier, as published by Microsoft and consulted October 2026. Microsoft Purview audit log retention policies. Establishes the 180 day standard retention of the Unified Audit Log and the licensing required for longer retention, as published by Microsoft and consulted October 2026. 18 U.S.C. 1030, Fraud and related activity in connection with computers. Supplies the statutory language on access without authorization that frames civil and criminal claims arising from account compromise, current text at Cornell LII. Federal Rule of Civil Procedure 37(e). Sets the reasonable steps standard against which preservation of expiring cloud logs is judged, current text at Cornell LII.

© 2026 Global Digital Forensics, Inc. All rights reserved.

FREQUENTLY ASKED

Password Resets, Sign In Logs and Revoked Sessions

Does resetting the password end a token based intrusion?

A reset is one step in the sequence. A password reset changes the credential used to obtain new tokens, while refresh and access tokens that were already issued may remain valid until they expire or are revoked, and a rogue application consent survives a reset entirely. The sequence matters: preserve the sign in and audit records first, then revoke sessions, remove unfamiliar authenticators and applications, and confirm in the logs that new sessions have stopped. We review that sequence with your administrators so containment and the evidence of how the intruder entered are both kept.

How long does Microsoft keep the sign in logs we would need?

Microsoft publishes the retention. Entra sign in logs are retained seven days on the free tier and thirty days with Premium P1 or P2 licensing, and the Purview Unified Audit Log is retained 180 days on the standard tier, and longer when the organization licensed and configured extended retention. If the tenant forwards logs to a SIEM or storage account, those copies may extend the window. We confirm the actual configuration on the first call because the answer sets the pace for preservation.

Can you tell which emails the attacker actually read?

Sometimes, and we are precise about how we say it. Mailbox auditing records MailItemsAccessed events that identify folders and, in some cases, individual items accessed by a session; the log aggregates and throttles when access volume is high, and a sync operation records what was downloaded, so the examiner reads item level events, where present, for what a person opened. The report distinguishes items the log affirmatively records from exposure we infer from folder level sync, and that distinction carries directly into the notification analysis counsel performs.

What drives the cost and timing of a token compromise analysis?

The number of affected identities, whether audit logging was enabled before the incident, whether the tenant has Premium licensing or a SIEM that extends retention, how many sessions and applications must be traced, and whether the deliverable is an internal report, a declaration or testimony. A single mailbox with intact logs is a narrower engagement than a tenant with privileged role changes and application consents. The initial consultation is free, and we scope the work in writing before any analysis begins.

Should our security team revoke sessions before you are engaged?

If funds or data are actively leaving, containment comes first and we work from the record as it stands. If the activity appears historical, export the sign in logs, audit log search results, inbox rules and application consents in native format before revoking anything, then revoke. Both paths are defensible when they are documented, and we help administrators record who did what and when so the containment steps become part of the evidence.

© 2026 Global Digital Forensics, Inc. All rights reserved.

Web Addresses for the Sources Cited

1. Entra data retention reference: https://learn.microsoft.com/en-us/entra/identity/monitoring-health/reference-reports-data-retention
2. published audit retention policies: https://learn.microsoft.com/en-us/purview/audit-log-retention-policies
3. data retention and lag times: https://support.google.com/a/answer/7061566
4. Federal Rule of Civil Procedure 37(e): https://www.law.cornell.edu/rules/frcp/rule_37
5. 18 U.S.C. 1030: https://www.law.cornell.edu/uscode/text/18/1030
6. NIST's September 2026 announcement on protecting online identity and access tokens: https://www.nist.gov/news-events/news/2026/09/nist-finalizes-guidelines-protecting-online-identity-and-access-tokens
7. Microsoft sign in documentation: https://learn.microsoft.com/en-us/entra/identity/monitoring-health/concept-sign-ins
8. Microsoft account compromise guidance: https://learn.microsoft.com/en-us/defender-office-365/responding-to-a-compromised-email-account
9. September 2026 identity compromise analysis: https://www.microsoft.com/en-us/security/blog/2026/09/09/passkey-themed-social-engineering-leads-identity-cloud-compromise/
10. mailbox auditing guidance: https://learn.microsoft.com/en-us/purview/audit-log-investigate-accounts

Reviewed by Joseph Caruso, Founder, CEO and CTO, CISSP. Last reviewed November 3, 2026.

Start With a Free Consultation

The initial consultation is free, and requests are handled in confidence. On the first call a senior member of our team listens to the question you need answered, identifies the records and systems involved, and recommends the next step.

Call (800) 868-8189, answered 24/7, request a consultation at evestigate.com/contact, or email info@evestigate.com.

© 2026 Global Digital Forensics, Inc. All rights reserved.