Global Digital Forensics · Guide edition 2026-11-03 · evestigate.com/insights/it-security-beware-a-cyber-security-nightmare-at-work-can-start-at-home/

HYBRID WORK SECURITY

How Infostealers on Home Office Devices Compromise Corporate Cloud Tenants

A stolen browser session from an employee's home computer walks past multi factor authentication and into the corporate cloud as a trusted user. Revoke the sessions, preserve the sign in and mailbox logs and keep the home machine as it is for the examiner. Call (800) 868-8189 at any hour.

Published September 8, 2015 · Updated October 30, 2026

Primary Reference for This Guide

Start with NIST SP 800-61 Revision 3, Incident Response Recommendations.

By Robert Knudsen, Computer forensics and cybersecurity examiner, Global Digital Forensics

How an Unmanaged Home Computer Bypasses Enterprise Security Investments

A corporation can spend millions of dollars hardening its office network and configuring enterprise laptops, yet leave the front door wide open if employees are permitted to log into corporate webmail, SharePoint, Citrix or VPN portals from unmanaged home desktop computers. When an employee or family member downloads a malicious browser extension, pirated software or a game mod on a home PC, commodity infostealer malware silently harvests every saved password and active browser session cookie stored in Chrome or Edge, handing criminal syndicates immediate, authenticated access to the employee corporate cloud session.

Enforcing Device Trust Boundaries and Conducting BYOD Forensic Examinations

Global Digital Forensics helps enterprise security leaders and legal counsel close the hybrid work gap. On the security side, our architects test conditional access policies and help organizations enforce strict device compliance checks so only managed, healthy corporate endpoints can access sensitive cloud tenants. When an incident or trade secret dispute involves an employee personal home computer or tablet, our forensic examiners work under counsel direction and agreed inspection protocols to image and analyze the personal device cleanly, isolating corporate artifacts and intrusion vectors while respecting personal privacy boundaries.

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

Reading a Session Hijack in the Identity and Mailbox Logs

A cookie stolen from a home PC produces a distinctive pattern in the tenant's own records, and reading that pattern is the first job. Microsoft Entra sign in logs separate interactive sign ins from non interactive token refreshes, and a replayed session typically appears as non interactive activity from a new IP address, a new autonomous system and an unfamiliar browser and operating system string, without a corresponding password or multi factor event. The device identifier is absent or differs from the employee's enrolled devices. The unified audit log then shows what the session did: MailItemsAccessed with a bind or sync type, SearchQueryInitiated entries that reveal what the intruder was looking for, inbox rule creation and modification operations that forward or hide mail, and consent grants to OAuth applications that persist after the password changes. Those records are where the examiner fixes the window of access and the scope of what was touched.

The home computer supplies the other half. Infostealer malware leaves its own evidence in the browser's Login Data and Cookies databases, in the Prefetch and Amcache records of the dropper, in the scheduled tasks or run keys that kept it alive and in the network connections to its command server. Matching the malware's execution time against the first anomalous sign in is how the examiner tests the link between the home device and the corporate intrusion, which matters for insurance, for the notification analysis and for any later dispute about where the failure occurred. Coverage is mapped with the same care. Where audit logging was never enabled or a license tier's retention has already run, the report records the period and the settings, and the examiner turns to the home device, backups and other sources for that stretch. We set out which questions the surviving records answer and where we look for the rest, so that the privacy and legal analysis rests on facts rather than on the worst case assumption.

Timing is the detail that ties it together. Entra sign in logs, the unified audit log, the home computer's event logs and the malware's own network connections each run on their own clock, and the report normalizes them to a single time zone with the offsets stated, so that the first malicious token refresh can be shown to follow the stealer's execution by minutes rather than appearing to precede it. That alignment is what lets counsel tell an insurer or a regulator exactly when the exposure began and ended. It also narrows the content assessment to the messages and files that existed in the mailbox during that window, which is usually far fewer than the whole, and it is the first thing an opposing expert or a regulator's technical reviewer will test.

Containment, Preservation and Analysis Sized for a Small Team

Most organizations hit by this scenario run with a small IT team rather than a security operations center watching the logs, so the response is sequenced for that team. Containment comes first and is specific: revoke all refresh tokens for the affected account, reset the password, review and remove unfamiliar inbox rules and OAuth consents, re register multi factor methods and, if conditional access is available, require a compliant device for the account. Preservation happens in the same hour. The sign in logs, the unified audit log for the account and any inbox rule history are exported before anyone tidies the mailbox, because remediation steps create their own events and can push older entries past export limits. The process follows NIST SP 800-61 Revision 3, which organizes incident response under the CSF 2.0 functions of govern, identify, protect, detect, respond and recover, adapted to a team of two or three.

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

Analysis then determines what the intruder saw and did, which is the question counsel and the privacy officer actually need answered. We reconstruct the session window, enumerate the messages and attachments accessed, identify searches run, trace any forwarding and look for lateral movement into SharePoint, Teams or other accounts through shared mailboxes and delegated permissions. The findings feed a content assessment of the exposed material, which the privacy incident technical support practice turns into the facts counsel need for state breach statutes and contractual notices. Our guide to suspected cloud session token theft covers the preservation list in detail, and the business email compromise analysis page describes the engagement when the intruder moved to payment fraud.

Examining a Personal Device Under an Inspection Protocol

The home computer belongs to the employee or a family member, and the examination has to respect that from the start. We work under an inspection protocol agreed between counsel and the device owner, or ordered by a court, that defines what the examiner may look at: the malware and its artifacts, the browser profiles that held corporate sessions and the time range of the incident. The device is imaged in full so the evidence is fixed, but the analysis is confined to the protocol's scope and the report documents that confinement. Personal photographs, finances and family communications stay closed, and the protocol usually names a neutral or counsel who resolves disputes about scope. This structure protects the employee's privacy and protects the company from a later claim that the examination was a pretext for something else.

Before the first call, the employee stops using the computer, leaves it powered on if it is on and off if it is off, disconnects it from the network and leaves it as it is. Keeping the suspicious extension, the browser data and the operating system in place preserves the records the examiner reads to determine what the malware took and when. The security team asks the employee to change personal passwords from a separate, trusted device, which keeps new credentials away from a stealer that may still be running. Counsel joins before the device is requested so that the request, the protocol and the handling of what is found are all coordinated. Our computer forensics practice handles the imaging and analysis, and Robert Knudsen leads the work.

Three Decisions That Keep an Incident Contained

The first decision is to revoke the refresh tokens alongside the password reset. A stolen session token keeps working through a reset, and revoking the refresh tokens is the step that ends the intruder's access to the mailbox; the logs pulled afterward are read to confirm when the activity stopped. The second is to follow the session across the whole account. Infostealer logs are sold in bulk, and the same home machine often held sessions for several corporate applications, so the analysis covers every system the employee could reach from that browser. The third is to preserve the mailbox before tidying it, which keeps the forwarding rules and the intruder's own messages that help define the scope. Together these decisions keep the notification analysis as narrow as the facts allow, because the privacy officer works from the record of what was accessed rather than from an assumption.

Prevention costs less, and the controls are familiar ones. Conditional access that requires a managed, compliant device for sensitive applications denies the replayed cookie a place to land. Token protection and shorter session lifetimes limit the value of what is stolen. Mailbox auditing turned on and retained for as long as the license allows gives the examiner something to read. Regular penetration testing of the remote access path tests whether the policies actually hold, and an incident response retainer means the examiner who

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

answers the call already knows the environment. For organizations that want the full picture of the exposure before an incident, our forensic readiness planning engagement maps the logs, the retention and the people who will act.

Audit Your Remote Access and Hybrid Work Boundaries

Call Global Digital Forensics at (800) 868-8189 to test your remote access conditional policies or coordinate a defensible remote device examination. Our guide to suspected cloud session token theft explains what to preserve when a stolen cookie is already in play. The initial consultation is free.

Reading a Session Hijack Across the Home PC and the Tenant

The guide explains that a cookie stolen from a home computer produces a distinctive pattern in the tenant records and leaves its own evidence on the home device. This table pairs each half of the record with what it shows and how it is retained and preserved, so a small team can contain and preserve in the same hour. The retention column sets the export schedule, and revoking sessions alongside the password reset is the step that ends a stolen token's use.

Records on the tenant side and the home device after a session hijack, what each shows and how it is retained and preserved.

Record	What it shows	Retention and preservation
Entra non interactive sign ins	A replayed token from a new address and browser	Retained seven or thirty days by license per Microsoft
Unified Audit Log	MailItemsAccessed, searches, rule and consent changes	Retained 180 days as standard per Microsoft
Home browser Login Data and Cookies	What the infostealer harvested	Preserved by keeping the machine as it is
Prefetch and Amcache on the home PC	The dropper and when it ran	Preserved by taking the machine out of use
Scheduled tasks and run keys	How the malware stayed alive	Preserved by leaving cleanup to the examiner
Malware network connections	The command server contacted	Captured from the preserved device
Clock alignment across sources	Whether the token refresh followed the stealer, and by how long	Each source's clock normalized to one time zone

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

How to Begin and What Happens on the First Call

Have ready the affected account names, the time the anomaly was noticed and how, what has already been done to the account and to the home computer, the identity platform and license tier in use and whether conditional access or mailbox auditing is enabled. The examiner asks whether sessions have been revoked, whether the audit logs have been exported, what the account could reach, who owns the home device and whether counsel is involved. You then receive a written scope describing the immediate containment and preservation steps, the log analysis, the device examination protocol if one is needed and the timing, with a proposal. The initial consultation is free, and the hotline at (800) 868-8189 answers 24/7.

Technical References and Further Reading

Authorities cited in this guide: NIST SP 800-61 Revision 3, Incident Response Recommendations and Considerations for Cybersecurity Risk Management. Provides the incident response life cycle and its alignment to the Cybersecurity Framework 2.0, final version published 2025. Microsoft Learn, Manage audit log retention policies. Documents how long Microsoft 365 sign in and mailbox audit records are kept by license level, current Microsoft documentation. 18 U.S.C. 1030, Fraud and related activity in connection with computers. Defines unauthorized access to a protected computer, the federal statute counsel most often cite when a stolen session is used, current codified text.

FREQUENTLY ASKED

Home Devices and Corporate Tenants

Can a stolen session cookie really bypass multi factor authentication?

Yes. Multi factor authentication is checked when the session is created. Once the identity provider issues the session and refresh tokens, the browser presents them on every request and the server trusts them until they expire or are revoked. Malware that copies the browser's cookie database copies those tokens, and an intruder who loads them into another browser is treated as the already authenticated user. The sign in logs usually reveal it through non interactive activity from an unfamiliar network and device, which is why revoking sessions alongside the password reset is the first containment step.

Can the company examine an employee's personal computer?

Yes, with the owner's consent or a court order, and in practice through an inspection protocol negotiated by counsel that limits the examination to the malware, the corporate sessions and the incident time frame. The company's interest is in understanding how its data was reached. The employee's interest is in keeping personal material private. A written protocol that names the scope, the examiner, the handling of the image and the resolution of disputes protects both, and the examination report documents that the agreed scope was observed.

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

How do we know whether other accounts or systems were reached?

By following the session rather than the user. The identity provider's logs show every application the token was used against, and the unified audit log shows activity in SharePoint, OneDrive, Teams and shared mailboxes under that identity. On the home computer, the stolen cookie database shows every other site where sessions were saved, which may include payroll, banking, customer portals and software as a service tools outside the tenant. We list each exposed application so that the security team can revoke sessions and the privacy analysis can account for every data set the session reached, the mailbox included.

Should we tell the employee what we found on their home computer?

That is a decision for counsel and HR, and it is usually shaped by the inspection protocol and by whether the malware came from the employee's own conduct or a family member's. Our role is to report facts within the protocol's scope: what the malware was, when it ran, what it collected and which corporate sessions it exposed. The report describes events and leaves blame out of it. In many of these matters the employee is a victim as well, and the factual report lets the company address the policy question, such as whether personal devices may reach corporate applications at all, on a factual footing.

What should the employee do with the home computer right now?

Stop using it, disconnect it from the network and set it aside. If it is powered on, leave it on so volatile evidence and running processes can be captured. Keep the machine as it is, with the extension, the browser data and the installed software in place, because those are the records the examiner reads to reconstruct what the malware did. Change corporate and personal passwords from a different, trusted device after the company has revoked the active sessions. Counsel and the examiner then arrange the collection under an agreed protocol.

Web Addresses for the Sources Cited

1. NIST SP 800-61 Revision 3, Incident Response Recommendations: https://csrc.nist.gov/pubs/sp/800/61/r3/final
2. Microsoft Learn, Manage audit log retention policies: https://learn.microsoft.com/en-us/purview/audit-log-retention-policies
3. 18 U.S.C. 1030, Fraud and related activity in connection with computers: https://www.law.cornell.edu/uscode/text/18/1030

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.