EXECUTIVE PROTECTION

The Open Browser Session Is Now What Attackers Try to Steal

When you sign in, the browser keeps proof that you have already identified yourself, as a cookie or a token, so it does not ask for your password and second factor on every visit. Anyone who copies that proof to another computer can enter the account as you, without the password and without the code from your phone.

On 16 July 2026, Microsoft published an analysis of ACR Stealer malware campaigns that its Defender Experts team observed between late April and mid-June. They began with a ClickFix lure: a fake verification check that tells the person to paste and run something on their own computer. According to Microsoft, the campaigns went after browser-stored credentials, cookies, authentication tokens and documents.

The analysis is on Microsoft’s security blog, 16 July 2026.
https://www.microsoft.com/en-us/security/blog/2026/07/16/acr-stealer-two-observed-intrusion-chains-amid-increased-threat-activity/

Why the Second Factor Does Not Stop This Theft

A second factor protects the moment you sign in, and a stolen session is used afterwards. That is why changing the password is not enough: for a suspected compromise, Microsoft recommends rotating exposed credentials and also revoking potentially compromised tokens. The opening trick is not rare either. As The Register reported on 16 October 2025, Microsoft’s Digital Defense Report 2025 said ClickFix was the most common initial access method in its Defender Experts notifications over the previous year, at 47% of attacks, against 35% for phishing.

The damage may not stay in one account. Help Net Security reported on 20 May 2026 that Verizon’s 2026 DBIR describes infostealers as a pipeline to ransomware: half of the ransomware victims who had a prior credential leak saw that leak within 95 days of the attack. The same report says vulnerability exploitation overtook stolen credentials as the most common initial access route for the first time: updates count too.

The DBIR findings were summarised by Help Net Security on 20 May 2026.
https://www.helpnetsecurity.com/2026/05/20/verizon-2026-dbir-findings/

What to Change on Devices and Accounts This Week

- Move passwords saved in the browser into a manager with its own unlock, then delete the browser's copies.
- Keep separate browser profiles for work, banking and personal use; you then know which sessions to end if something goes wrong, although malware on the computer can reach every profile.
- Install system and browser updates as soon as they come out, on the executive's computer and on their assistant's.
- Agree a rule with no exceptions: no legitimate page, email or support person asks you to paste and run something to verify yourself, and if it happens, the tab is closed and someone is told.
- Turn on passkeys wherever a service offers them, starting with email and administration accounts, and check that the recovery method still works.

Two recent defences help, within limits. Google announced on 28 May 2026 that Device Bound Session Credentials (DBSC) had become generally available in Chrome on Windows, on by default for Google Workspace and available to personal accounts too: it binds the session cookie to the device where you signed in and, according to Google, reduces the risk of session theft even if malware is present. It covers only Google sessions in Chrome on Windows. The FIDO Alliance's Passkey Index 2026, published on 15 October with data from 15 participating services, reports that on average 36% of successful sign-ins at those services now use a passkey, and that passkey sign-ins succeed more often than those using passwords and traditional multi-factor authentication (93% against 78%). Those are figures for the participants, not the internet as a whole, and a passkey protects the sign-in, not the session left open afterwards.

The DBSC announcement is on the Google Workspace Updates blog, 28 May 2026.
https://workspaceupdates.googleblog.com/2026/05/prevent-account-takeovers-with-DBSC-now-generally-available-in-the-Chrome-browser-for-Windows.html

If You Suspect an Infection, Act in This Order

- First, take the suspect computer off the network and, from another trusted device, end every session and revoke tokens and app access for email, cloud storage, banking and social accounts.
- Straight after, change the passwords, starting with the email that recovers the others, and do not use the suspect computer to sign in anywhere until it has been checked or reinstalled.
- Next, review recovery methods, forwarding rules, email filters and connected apps, because that is where someone could leave a way back in.

- Tell whoever manages the company’s systems and keep the alerts you received.

How Executive Digital Protection Does It

We review the executive’s and their assistant’s computers: which passwords each browser stores, which profiles and extensions exist, whether everything updates, and whether command tools should be restricted on machines used for non-technical work. We move passwords into a manager with its own recovery plan and turn on passkeys where they are supported. On the accounts, we review sessions, connected apps, forwarding rules, recovery and sign-in alerts. We write down the incident routine, with who runs it and from which device, and rehearse it without closing the access that works. Depending on the plan, we monitor for leaks of the executive’s email addresses and domains so sessions can be ended and passwords changed when they appear.

> *These measures reduce the likelihood and reach of session theft but do not remove it. DBSC, passkeys and session revocation depend on what each provider offers, and leak monitoring only finds what appears in the sources it covers.*

A Check You Can Run

Open your Google Account, go to Security & sign-in and, under Your devices, select Manage all devices. Go through each device and session and ask whether you recognise the device, the browser and the place. A recent trip, a new phone or an approximate location explains many differences. Sign out of any session you are not sure is yours, from a device you trust. While you are there, note how many passwords each browser you use still stores: that list is the starting point for moving them into a manager.

Supporting guidance: Google’s instructions for reviewing devices with account access.
https://support.google.com/accounts/answer/3067630?hl=en

Continue with: A Password Manager Needs a Recovery Plan Too.
https://systems.kavaliero.com/en/blog/a-password-manager-needs-a-recovery-plan-too

For help with this work, see the scope of Executive Digital Protection.
https://systems.kavaliero.com/en/services/executive-security