BLINDAJE EJECUTIVO

La Sesión Abierta del Navegador Es lo que Ahora Intentan Robar

Cuando inicias sesión, el navegador guarda una prueba de que ya te identificaste, en forma de cookie o de token, para no pedirte la contraseña y el segundo factor en cada visita. Quien copie esa prueba a otro equipo puede entrar a la cuenta como si fueras tú, sin la clave y sin el código del teléfono.

El 16 de julio de 2026, Microsoft publicó un análisis de campañas del malware ACR Stealer que su equipo Defender Experts observó entre finales de abril y mediados de junio. Empezaban con un señuelo de tipo ClickFix: una falsa comprobación de verificación que pide a la persona pegar y ejecutar algo en su propio equipo. Según Microsoft, buscaban credenciales guardadas en el navegador, cookies, tokens de autenticación y documentos.

El análisis está publicado en el blog de seguridad de Microsoft del 16 de julio de 2026.
https://www.microsoft.com/en-us/security/blog/2026/07/16/acr-stealer-two-observed-intrusion-chains-amid-increased-threat-activity/

Por Qué el Segundo Factor No Frena Este Robo

El segundo factor protege el momento de entrar, y una sesión robada se usa después. Por eso cambiar la contraseña no basta: ante un posible compromiso, Microsoft recomienda rotar las credenciales expuestas y, además, revocar los tokens que puedan estar comprometidos. El engaño inicial tampoco es raro. Según reportó The Register el 16 de octubre de 2025, el Digital Defense Report 2025 de Microsoft indicó que ClickFix fue el método de acceso inicial más común en las notificaciones de Defender Experts del año anterior, con el 47% de los ataques, frente al 35% del phishing.

El daño puede no quedarse en una cuenta. Help Net Security informó el 20 de mayo de 2026 que el DBIR 2026 de Verizon describe los infostealers como una vía hacia el ransomware: la mitad de las víctimas de ransomware que habían sufrido una filtración previa de credenciales la tuvo dentro de los 95 días anteriores al ataque. El mismo informe señala que la explotación de vulnerabilidades superó por primera vez al robo de credenciales como la vía de acceso inicial más común: las actualizaciones también cuentan.

Los hallazgos del DBIR los resumió Help Net Security el 20 de mayo de 2026.
https://www.helpnetsecurity.com/2026/05/20/verizon-2026-dbir-findings/

Qué Cambiar Esta Semana en Equipos y Cuentas

- Pasa las contraseñas guardadas en el navegador a un gestor con su propio desbloqueo y borra después las copias del navegador.
- Separa perfiles de navegador para el trabajo, la banca y lo personal; así sabes qué sesiones cerrar si algo falla, aunque un programa malicioso en el equipo puede alcanzar todos los perfiles.
- Instala las actualizaciones del sistema y del navegador en cuanto salgan, en el equipo del ejecutivo y en el de su asistente.
- Acuerda una regla sin excepciones: ninguna página, correo o persona de soporte legítima te pide pegar y ejecutar algo para verificarte, y si ocurre, se cierra la pestaña y se avisa.
- Activa llaves de acceso (passkeys) donde el servicio las ofrezca, empezando por el correo y las cuentas de administración, y comprueba que el método de recuperación sigue funcionando.

Dos defensas recientes ayudan, con límites. Google anunció el 28 de mayo de 2026 que Device Bound Session Credentials (DBSC) pasó a disponibilidad general en Chrome para Windows, activado por defecto en Google Workspace y disponible también para cuentas personales: vincula la cookie de sesión al equipo donde entraste y, según Google, reduce el riesgo de robo de sesión aunque haya malware en el equipo. Solo cubre sesiones de Google en Chrome sobre Windows. El Passkey Index 2026 de la FIDO Alliance, publicado el 15 de octubre con datos de 15 servicios participantes, indica que en promedio el 36% de los inicios de sesión exitosos en ellos ya usa una llave de acceso, y que estos salen bien más a menudo que los hechos con contraseña y autenticación multifactor tradicional (93% frente a 78%). Son cifras de esos participantes, no de internet en general, y una llave de acceso protege la entrada, no la sesión que queda abierta.

El anuncio de DBSC está en el blog de novedades de Google Workspace del 28 de mayo de 2026.
https://workspaceupdates.googleblog.com/2026/05/prevent-account-takeovers-with-DBSC-now-generally-available-in-the-Chrome-browser-for-Windows.html

Si Sospechas una Infección, Actúa en Este Orden

- Primero, desconecta de la red el equipo sospechoso y, desde otro de confianza, cierra todas las sesiones y revoca tokens y accesos de aplicaciones en el correo, la nube, la banca y las redes.
- Enseguida cambia las contraseñas, empezando por el correo que recupera las demás, y no uses el equipo sospechoso para entrar a ninguna cuenta hasta que se revise o se reinstale.
- Luego revisa métodos de recuperación, reglas de reenvío, filtros del correo y aplicaciones

conectadas, porque ahí alguien podría dejar una vía para volver.

- Avisa a quien administra los sistemas de la empresa y conserva las alertas recibidas.

Cómo lo Hace Blindaje Ejecutivo

Revisamos los equipos del ejecutivo y de su asistente: qué claves guarda cada navegador, qué perfiles y extensiones hay, si todo se actualiza y si conviene restringir las herramientas de comandos en equipos de uso no técnico. Pasamos las claves a un gestor con su plan de recuperación y activamos llaves de acceso donde se admiten. En las cuentas, revisamos sesiones, aplicaciones conectadas, reglas de reenvío, recuperación y alertas de inicio de sesión. Dejamos por escrito la rutina de incidente, con quién la ejecuta y desde qué equipo, y la ensayamos sin cerrar los accesos que funcionan. Según el plan, vigilamos filtraciones de los correos y dominios del ejecutivo para cerrar sesiones y cambiar claves cuando aparecen.

> *Estas medidas reducen la probabilidad y el alcance de un robo de sesión, pero no lo eliminan. DBSC, las llaves de acceso y la revocación de sesiones dependen de lo que ofrezca cada proveedor, y la vigilancia de filtraciones solo encuentra lo que aparece en las fuentes revisadas.*

Una Comprobación Concreta

Abre tu cuenta de Google, entra en la sección de seguridad e inicio de sesión y, en Tus dispositivos, elige ver todos los dispositivos. Revisa cada equipo y cada sesión y pregúntate si reconoces el dispositivo, el navegador y el lugar. Un viaje reciente, un teléfono nuevo o una ubicación aproximada explican muchas diferencias. Cierra, desde un equipo de confianza, cualquier sesión de la que no estés seguro. Aprovecha para anotar cuántas contraseñas guarda todavía cada navegador que usas: esa lista es el punto de partida para pasarlas a un gestor.

Documentación de apoyo: Instrucciones de Google para revisar los dispositivos con acceso a la cuenta.
https://support.google.com/accounts/answer/3067630?hl=en

Para seguir leyendo: Un Gestor de Contraseñas También Necesita un Plan de Recuperación.
https://systems.kavaliero.com/blog/un-gestor-de-contrasenas-tambien-necesita-un-plan

Si necesitas ayuda con este trabajo, consulta el alcance de Blindaje Ejecutivo.
https://systems.kavaliero.com/soluciones/blindaje-digital