AIRNITE

ZERO DAY

NÚMERO 09/2026 · MARKETING Y SEO

El anuncio del anuncio: así secuestran los estafadores cuentas de Google Ads

Unos delincuentes publican anuncios de Google que se hacen pasar por Google Ads y así roban las cuentas publicitarias de empresas, presupuesto incluido. Cómo funciona la estafa y cómo protegerse como anunciante.

Publicado: 21 de noviembre de 2026 Tiempo de lectura: 5 min Autor: Redacción de Airnite

SOFTWARE. SECURITY. CODE.

// LA SITUACIÓN EN CIFRAS

sites.google.com
camuflaje de la página de phishing
falsa página de inicio de Google Ads en Google Sites (Malwarebytes)

+1 admin
nuevo administrador en la cuenta
añadido con otra dirección de Gmail (Malwarebytes)

3
campañas observadas
grupos de Brasil y Asia, un tercero quizá de Europa del Este (Malwarebytes)

50+
anuncios fraudulentos denunciados
comunicados a Google por Malwarebytes en pocos días

Quien anuncia su empresa suele buscar rápido «Google Ads» en Google y pulsar el primer resultado. En eso confiaban precisamente los delincuentes sobre los que informó la empresa de seguridad Malwarebytes en enero de 2025: publicaban anuncios de búsqueda de pago que se hacían pasar por Google Ads y con ellos robaban las cuentas publicitarias de empresas.

// ¿Qué ha pasado?

Según Malwarebytes, los falsos anuncios «patrocinados» llevaban a una página que parecía la de inicio de Google Ads, pero estaba alojada en **Google Sites** y redirigía a un kit de phishing. Allí las víctimas introducían sus credenciales. Malwarebytes calificó la campaña como la operación de malvertising más grave que había seguido nunca y comunicó a Google **más de 50 anuncios fraudulentos** en pocos días.

Según Malwarebytes, detrás de la estafa hay al menos dos grupos principales: uno de habla portuguesa de Brasil, con diferencia el más activo según sus observaciones, y otro de Asia que usaba cuentas publicitarias de Hong Kong. Una tercera campaña, quizá de Europa del Este, recurría a un CAPTCHA falso y a un señuelo de Google Authenticator.

// ¿Cómo funciona el ataque?

El truco aprovecha la confianza por partida doble: en los resultados de Google y en el dominio de Google. Como la página de phishing estaba en sites.google.com, la dirección del anuncio parecía auténtica. Según Malwarebytes, el kit recogía nombres de usuario, contraseñas, cookies y un identificador único.

Con esos datos, los autores iniciaban sesión y añadían a la cuenta publicitaria un **nuevo administrador** con otra dirección de Gmail. Después podían publicar sus propios anuncios con el presupuesto de la víctima, a menudo más anuncios fraudulentos, y dejar fuera al titular legítimo. Según Malwarebytes, los grupos buscan revender las cuentas. Una cuenta publicitaria con un medio de pago guardado es dinero contante para los delincuentes.

// ¿A quién afecta?

Afecta a empresas, agencias y autónomos que usan Google Ads, desde la pequeña tienda online hasta la gran empresa. El daño es doble: el presupuesto se gasta en anuncios ajenos y es posible que circule un fraude con su nombre, lo que perjudica su reputación. A eso se suma el esfuerzo de recuperar la cuenta.

El patrón va más allá de Google Ads. Cualquier plataforma cuya página de acceso se «busca rápido en Google» es un objetivo: cuentas publicitarias, banca online, servicios en la nube, marketplaces.

// ¿Qué hay que hacer ahora?

La regla más importante es sencilla: no abra nunca páginas de acceso desde un anuncio, siempre desde un marcador. Añada autenticación multifactor, revisiones periódicas de los usuarios de la cuenta y alertas que no se pierdan en la bandeja de entrada. Los presupuestos limitados hacen que un abuso se detecte pronto y quede acotado. La lista de control de abajo resume los pasos.

// ¿Cómo ayuda Airnite?

Airnite gestiona **campañas SEA** y protege las cuentas desde el principio: funciones, permisos, autenticación multifactor, alertas y límites de presupuesto. En la **formación**, los equipos de marketing aprenden a reconocer el phishing con anuncios y las páginas de acceso falsas. Con **pruebas de penetración** comprobamos lo bien protegidas que están sus cuentas y accesos frente a intentos de toma de control.

> Nota: la base es sobre todo el informe de Malwarebytes, que no incluye ninguna declaración de Google. Estado de la investigación: 21 de noviembre de 2026.

Lista de control: qué hacer ahora

[+] Abra Google Ads solo desde un marcador o escribiendo la dirección, nunca desde un anuncio en los resultados de búsqueda.

[+] Compruebe la barra de direcciones antes de cada inicio de sesión: los accesos reales a Google Ads no pasan por sites.google.com.

[+] Active la autenticación multifactor en todas las cuentas con acceso, idealmente con llaves de seguridad.

[+] Revise con regularidad los usuarios y administradores de la cuenta y elimine de inmediato cualquier acceso desconocido.

[+] Haga que las alertas de inicio de sesión y de cambios lleguen a varias personas responsables, y tómelas en serio.

[+] Limite los presupuestos diarios y de la cuenta y elija medios de pago que permitan detectar rápido un abuso.

Cómo ayuda Airnite

- SEA – publicidad de pago – Anuncios en Google y Amazon que salen rentables.
- Formación – Su equipo aprende nuestras herramientas y procesos.
- Pruebas de penetración y seguridad – Ataques controlados con un informe claro y un plan de medidas.

¿Está su cuenta publicitaria tan protegida como su cuenta bancaria?

Airnite gestiona sus campañas de Google Ads y a la vez protege la cuenta: autenticación multifactor, funciones y permisos ordenados, alertas ante cambios y límites de presupuesto. Ante cualquier sospecha, revisamos de inmediato la cuenta y los accesos.

Solicitar una primera conversación · Escribir un correo · Por WhatsApp

Contacto

¿Preguntas sobre este artículo? Escríbanos por WhatsApp: +49 174 6834842

Leer en línea: https://airnite.de/es/revista/cuentas-google-ads-secuestradas-malvertising/

Fuentes

Cada dato de este artículo se basa en las fuentes indicadas a continuación. Las fuentes primarias están señaladas.

1. **Malwarebytes · The great Google Ads heist: criminals ransack advertiser accounts via fake Google ads** · 15/01/2025 · FUENTE PRIMARIA
   Investigación de seguridad (informe original): desarrollo, phishing con Google Sites, nuevos administradores, grupos
   https://www.malwarebytes.com/blog/news/2025/01/the-great-google-ads-heist-criminals-ransack-advertiser-accounts-via-fake-google-ads

2. **BleepingComputer · Hackers use Google Search ads to steal Google Ads accounts** · 2025
   Prensa especializada: contexto de la campaña
   https://www.bleepingcomputer.com/news/security/hackers-use-google-search-ads-to-steal-google-ads-accounts/

Información editorial general, no constituye asesoramiento jurídico ni una evaluación de sus sistemas concretos. Vigencia: fecha de publicación.

Airnite GmbH · Am Waldbach 7 · 77654 Offenburg · airnite.de