AIRNITE

# ZERO DAY

ISSUE 09/2026 · MARKETING & SEO

# The ad for the ads: how fraudsters hijack Google Ads accounts

Criminals run Google ads posing as Google Ads and use them to steal companies' advertising accounts – budget included. How the scam works and how advertisers can protect themselves.

Published: 21 November 2026 Reading time: 5 min Author: Airnite editorial team

SOFTWARE. SECURITY. CODE.

// THE SITUATION IN NUMBERS

**sites.google.com**
**disguise of the phishing page**
fake Google Ads home page on Google Sites (Malwarebytes)

**+1 admin**
**new administrator in the account**
added via a different Gmail address (Malwarebytes)

**3**
**campaigns observed**
groups from Brazil and Asia, a third possibly Eastern Europe (Malwarebytes)

**50+**
**fraudulent ads reported**
reported to Google by Malwarebytes within a few days

Anyone advertising a business often quickly searches Google for “Google Ads” and clicks the first result. That is exactly what the criminals reported by security firm Malwarebytes in January 2025 relied on: they ran paid search ads posing as Google Ads – and used them to steal companies' advertising accounts.

## // What happened?

According to Malwarebytes, the fake “sponsored” ads led to a page that looked like the Google Ads home page but was hosted on **Google Sites** and redirected to a phishing kit. There, victims entered their credentials. Malwarebytes called the campaign the most egregious malvertising operation it had ever tracked and reported **more than 50 fraudulent ads** to Google within a few days.

According to Malwarebytes, at least two main groups are behind the scam: a Portuguese-speaking group from Brazil, by far the most prolific according to its observations, and a group from Asia using advertiser accounts from Hong Kong. A third campaign, possibly from Eastern Europe, used a fake CAPTCHA and a Google Authenticator lure.

## // How does the attack work?

The trick exploits trust twice: in Google's search results and in the Google domain. Because the phishing page sat on sites.google.com, the address shown in the ad looked genuine. According to Malwarebytes, the phishing kit collected usernames, passwords, cookies and a unique identifier.

With the stolen data, the perpetrators logged in and added a **new administrator** to the ad account via a different Gmail address. They could then run their own ads on the victim's budget – often more scam ads – and lock out the rightful owner. According to Malwarebytes, the groups aim to resell the accounts. An ad account with a stored payment method is cash for criminals.

## // Who is affected?

Companies, agencies and freelancers using Google Ads are affected – from small online shops to large corporations. The damage is twofold: the budget is spent on someone else's ads, and fraud may run under your own name, harming your reputation. On top of that comes the effort of regaining the account.

The pattern goes beyond Google Ads. Every platform whose login page people “just quickly google” is a target: ad accounts, online banking, cloud services, marketplaces.

## // What should you do now?

The most important rule is simple: never open login pages via a search ad, always via a bookmark. Add multi-factor authentication, regular checks of the users in the account and alerts that do not get lost in the inbox. Capped budgets make sure misuse is noticed quickly and stays small. The checklist below sums up the steps.

## // How does Airnite help?

Airnite manages **SEA campaigns** and secures the accounts from the start: roles, rights, multi-factor authentication, alerts and budget limits. In **training**, marketing teams learn to recognise phishing via ads and fake login pages. With **penetration tests**, we check how well your accounts and access are protected against takeover attempts.

> Note: the basis is mainly the Malwarebytes report; it does not include a statement from Google. Research status: 21 November 2026.

## Checklist: what to do now

[+] Open Google Ads only via a bookmark or by typing the address – never via an ad in search results.

[+] Check the address bar before every login: genuine Google Ads logins do not run through sites.google.com.

[+] Enable multi-factor authentication for every account with access, ideally with security keys.

[+] Review users and administrators in the account regularly and remove unknown access immediately.

[+] Have login and account change alerts sent to several responsible people – and take them seriously.

[+] Cap daily and account budgets and choose payment methods so that misuse is noticed quickly.

## How Airnite helps

- SEA – paid advertising – Ads on Google and Amazon that pay off.
- Training – Your team learns our tools and processes.
- Penetration Testing & Security – Controlled attacks with a clear report and action plan.

## Is your ad account as secure as your bank account?

Airnite manages your Google Ads campaigns and secures the account at the same time: multi-factor authentication, clean roles and access rights, alerts on changes and budget limits. If anything looks suspicious, we check the account and access immediately.

**Request an initial call · Send an email · Via WhatsApp**

## Contact

Questions about this article? Message us on WhatsApp: +49 174 6834842

Read online: https://airnite.de/en/magazine/google-ads-accounts-hijacked-malvertising/

# Sources

Every fact in this article is based on the sources below. Primary sources are marked.


1. **Malwarebytes · The great Google Ads heist: criminals ransack advertiser accounts via fake Google ads** · 15 Jan 2025 · PRIMARY SOURCE
   Security research (original report): sequence, phishing via Google Sites, new administrators, groups
   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
   Trade press: context of the campaign
   https://www.bleepingcomputer.com/news/security/hackers-use-google-search-ads-to-steal-google-ads-accounts/


*General editorial information, not legal advice and not an assessment of your individual systems. Status: date of publication.*


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