Back button hijacking in Google's spam policies: what the new FAQ says

25 November 2026 · 5 min read · blogs.iictp.org/back-button-hijacking-spam-policy-faq-google-search-explained

Short answer: Google Search Central added a FAQ on 23 November 2026 to the back button hijacking section of its spam policies. The policy defines back button hijacking as a site interfering with browser navigation by manipulating history or other functions so users cannot immediately return to the page they came from. The FAQ says site owners can still import advertising code, that Google acts only on pages that show the behaviour, and that the policy covers Discover and visits arriving from outside Search.

TL;DR The short version

- Google added an FAQ on 23 November 2026 to the back button hijacking section of its spam policies.
- Back button hijacking means manipulating browser history so people cannot return straight to the page they came from; Google acts only on pages that show it, including from Discover and outside Search.
- Site owners can still use advertising code, but should test key landing pages from search, social and Discover by pressing back once.

Read online, listen to it, or change the text size: https://blogs.iictp.org/back-button-hijacking-spam-policy-faq-google-search-explained

What is back button hijacking?

Google's spam policies define it as a site interfering with navigation by manipulating the browser history or other functionality so that people cannot use the back button to get straight back to the page they came from. It sits in the malicious practices part of the spam policies, according to Google's documentation update.

How the FAQ answers common questions

- **Third-party advertising code:** the FAQ notes some hijacking was caused by advertising platforms, and says site owners can keep working with them and importing their hosted code. Google says it takes action only on pages that exhibit the behaviour.
- **Reporting:** users can report potential spammy behaviour.
- **Discover:** the policy applies, because Discover is part of Google Search.
- **Other traffic sources:** if the hijacking happens while a user browses within a browser, the policy applies even when they arrived from a non-Search channel such as social media.
- **Open in app:** app navigation and "open in app" behaviour are outside the scope of the policy.

What is new

The new part is clarification, not a new rule: the FAQ explains scope. The documentation update log lists it as an FAQ section added on 23 November 2026 to answer common questions Google received about the policy.

What the documentation does not say

- It does not give a ranking effect size or a timeline for enforcement.
- It does not list specific scripts or vendors.
- I did not read a statement here on how a manual action or a ranking demotion is applied; check the spam policies page and Search Console messages for that.

How to check your own site

1. Open key landing pages from a search result, then press the browser back button once. Do you return to the results page?
2. Repeat from a social link and from a Discover card, because the policy covers those visits.
3. Audit third-party scripts (ad, consent, popup, recommendation widgets) for code that pushes extra history entries.
4. Remove or reconfigure anything that does, and re-test in several browsers and on mobile.

What it means for SEO and site owners

Navigation integrity is now an explicit policy topic, so a script that “traps” users after a click can become a search problem, not only a user-experience problem. Because the FAQ says advertising code is allowed unless it causes the behaviour, the test is the behaviour on the page, not the vendor. Sources were read on 25 November 2026. Products, rules and standards change, so check the linked originals before you rely on any detail.

Frequently asked questions

- **What is back button hijacking?** Manipulating browser history or functionality so users cannot immediately go back to the previous page.
- **Can I still use ad platform code?** Yes, according to the FAQ; Google acts only on pages that exhibit the behaviour.
- **Does it apply to Discover?** Yes, Discover is part of Google Search.
- **Does it cover “open in app” links?** The FAQ says app navigation and open-in-app behaviour are outside the policy.

Related reading

- How to identify Google Search traffic in analytics
- Google Ads invalid traffic overview card
- Certified Technical Practitioner

Related credential: Certified Technical Practitioner. Explore the exam facts and syllabus.

Sources and further reading

1. Google Search Central. Spam policies for Google web search (back button hijacking FAQ). Read 25 November 2026. developers.google.com/search/docs/essentials/spam-policies
2. Google Search Central. Latest documentation updates (entry dated 23 November 2026). developers.google.com/search/updates

Published by IICTP, an independent technical credential body, on 25 November 2026. The current version of this post is at https://blogs.iictp.org/back-button-hijacking-spam-policy-faq-google-search-explained. More guides: blogs.iictp.org.