

How do I know if my site is hacked?

Follow these steps if:

- You've been alerted by Google that your site is hacked
- You see a warning in search that your site is hacked or compromised
- You're not sure if your site is actually hacked

If you're unsure if your site is actually hacked, or if you think your site was incorrectly flagged, start by registering your site in [Search Console](#). Go to the [Manual Actions](#) or the [Security Issues](#) sections of Search Console and look for example URLs where Google detected that your site has been hacked.

If you're unable to see hacked content on the URLs provided in Search Console, the hacked content might be using a technique known as [cloaking](#). Cloaking makes cleaning a site more difficult by showing different content to different types of users. For example, when you go to a page on your site like `www.example.com/cheap-drugs`, you might see a page without any content. This might lead you to believe that the hacked content on your site doesn't exist. However, when a search engine like Google accesses `www.example.com/cheap-drugs`, it will see spammy words and links.

To check for cloaking, use the [Hacked Sites Troubleshooter](#). The troubleshooter will walk you through a few tools like the `site:` search operator and [Fetch as Google](#) that can help you uncover any cloaked hacked content.

After you've double checked your pages, if you still think think your site was incorrectly flagged, please post in the [Webmaster Help Forums](#). Otherwise, start building your [support team](#).

[Previous](#)



[Overview](#)

[Next](#)

[Build a support team](#)



Except as otherwise noted, the content of this page is licensed under the [Creative Commons Attribution 3.0 License](#), and code samples are licensed under the [Apache 2.0 License](#). For details, see our [Site Policies](#). Java is a registered trademark of Oracle and/or its affiliates.

Last updated December 22, 2017.