Request a review

You must request a review from Google to have your page or site unflagged as dangerous or possibly deceptive to users.

You'll need

- Knowledge of shell/terminal commands

What you'll do

1. Prerequisites

Before requesting a review, confirm that you've taken the following steps:

- Verified ownership of your site in Search Console
- Cleaned your site of the hacker's vandalism
- Corrected the vulnerability
- Brought your clean site back online

2. Double-check that your pages are available and clean

To be safe, use either Wget or cURL to view pages on your site, such as your homepage and a URL modified by the hacker; these should now be clean. If so, and you're confident that same applies to the rest of the pages on your site, it's time to request a review.

Note: Your pages must be available to be crawled by Googlebot to ensure that they are clean. Make sure that they are not roboted out or blocked from indexing by `noindex` robots META tags or directives.

3. Request a review

Before requesting a review:

- **be sure that the problem is truly fixed**; requesting a review if the problem still exists will only prolong the period of time that your site is flagged as dangerous.
- **double-check where you should request a review**; the review process will take place in a specific tool, depending on the issue your site is facing. Please refer to the channels below.

A. Hacked site

*You received a hacked site notification in the **Manual Actions report** of the Search Console:*

1. Now that you have gone through the successive steps of the clean-up process, you can go in the Manual Actions report again and find the issue either as a site-wide match, or as a partial match.
2. Select **Request a review**.

   In order to submit a review, we ask that you provide more information on what you did to clean the site. For each category of hacked spam, you can write a sentence explaining how the site was cleaned (for example, "For Content injection hacked URLs, I removed the spammy content and corrected the vulnerability: updating an out-of-date plugin.").

B. Unwanted software (including malware)

*You received a malware or unwanted software notification in the **Security Issues report** of the Search Console:*

1. Open the **Security Issues report** again in Search Console. The report may still show the warnings and sample infected URLs you saw before.
2. Select **Request a review**.

   In order to submit a review, we ask that you provide more information on what you did to remove the policy violation from your site. For example, "I removed the 3rd-party code that was distributing malware on my website and replaced it with a more modern version of the code".

*You did not receive a malware or unwanted software notification in the **Security Issues report** of the Search Console, but you received a notification in your AdWords account:*

1. Request a review through the AdWords support center.

C. Phishing or Social Engineering

*You received a phishing notification in the **Security Issues report** of the Search Console:*

1. Open the **Security Issues report** again in Search Console. The report may still show the warnings and sample infected URLs you saw before.
2. Select **Request a review**.

   In order to submit a review, we ask you to provide more information on what you did to remove the policy violation from your site. For example, "I removed the page that was asking users to enter personal information".
3. You can also request the review at google.com/safebrowsing/report_error/. On top of serving as a reporting tool for site owners who believe their page was incorrectly flagged for phishing, this report will trigger a review of phishing pages that have been cleaned to lift warnings.

4. Wait for the review to be processed

- **Hacked with spam review process time:** Reviews for sites hacked with spam may require up to several weeks to process. This is because spam reviews can involve manual investigation or a complete reprocessing of the hacked pages. If the review is approved, Security Issues will no longer display hacked category types or example hacked URLs.
- **Malware review processing time:** Reviews for sites infected with malware require a few days to process. Once the review is completed, the response will be available within your **Messages** in Search Console.
- **Phishing review processing time:** Phishing reviews take about a day to process. If successful, the user-visible phishing warning will be removed and your page may again surface in search results.

If Google finds that your site is clean, warnings from browsers and search results should be removed within 72 hours.

If Google determines that you have not fixed the problem, the Security Issues report in Search Console could display more sample infected URLs to assist your next investigation for example. Malware, phishing or hacked with spam site warnings will remain in search results and/or browsers as a caution to protect users.

Final steps

- **If your request was approved,** verify that your site works as expected: pages load properly and links are clickable. To keep your site safe, we encourage all site owners to implement the maintenance and security plan created in Clean and maintain your site.

  For more information, consider the following resources from StopBadware:

  - Preventing badware: basics
  - Additional resources: hacked sites

- **If your request wasn't approved,** reassess your site for malware or spam, or for any modifications or new files created by the hacker. Alternatively, you can consider requesting more help from specialists in your support team.

Previous
← Clean and maintain your site

Last updated February 9, 2018.