Use Search Console

- You'll need
- What you'll do
  - Verify ownership of your site in Search Console {: #verify }
  - Check that the hacker didn't already verify ownership {: #check }
  - Determine the nature of the attack {: #determine }

{% YouTube "jC7jja6ebBM" %}

If you've already verified ownership of your site, you can skip the first action below and go right to checking your site information in Search Console.

You'll need

- The ability to verify ownership of your site using a technique such as adding a file in the root directory, authoring of `meta` tags, owning a Google Analytics administrative account for the site, etc.

What you'll do

In this section, you'll perform the following actions:

1. Verify ownership of your site in Search Console.
2. Check that the hacker didn't already verify ownership in Search Console and make unwanted settings changes.
3. Determine the nature of the attack.

Verify ownership of your site in Search Console {: #verify }

1. Open a browser and navigate to Webmaster Central.
2. Click **Search Console**.
3. Sign in to Search Console using a Google account. If you don't have a Google account, click **Create an account**. A new Google account doesn't mean you'll lose your existing email account with another company. (More information about accounts.)
4. Click **Add a site**. Type your site's URL in the box, then click **Continue**.
5. Decide the most convenient verification method for you. The **Recommended method** tab on the verification page shows the method Google thinks will work best. Additional methods are listed on the **Alternate methods** tab. (More information about verification.)
6. Bring your site back online if you selected a verification method that requires access to your site, such as HTML meta tag or HTML file.
7. Click **Verify** to verify ownership using your selected method. If verification is successful, you'll see a congratulatory screen mentioning that you're a verified owner. You can take your site back offline, but be aware that it will need to be back online in future steps.

Check that the hacker didn't already verify ownership {: #check }

Once verified, check that the hacker didn't already verify ownership in Search Console and make unwanted settings changes.

1. Navigate to the main Search Console homepage by clicking the Search Console logo.
2. Find your site, then click **Manage site.**
3. Click **Add or remove users**.
4. Be sure that all users and owners listed are authorized.
5. Document the email address of any unauthorized user (in case it's helpful in the future), then delete the user from your site. For unauthorized owners, you'll need to both delete the owner and any possible verification tokens, such as a verification metatag on your homepage or a HTML file on your server. (More information.)
6. Investigate for unwanted settings changes in Search Console. Click the settings Settings icon, then click **Site Settings** to check for possible undesirable changes by the hacker such as a lower Crawl rate (perhaps with the goal to avoid search engine spiders). Also, check that nothing unusual is listed in the section **Google Index** > Remove URLs or settings > Change of Address.

Determine the nature of the attack {: #determine }

The information in the Message Center and Security Issues in Search Console can help you determine whether your site was compromised in any of the following ways:

- With spammy content that could reduce the quality and relevance of search results.
- For phishing purposes.
- To distribute malware.

To investigate hacking or malware using Search Console, complete the following steps:

1. Navigate to the Search Console homepage by clicking the Search Console logo in the upper corner.
2. Click **Messages**.
3. Check if there is are any critical messages from Google regarding whether your site was used for 1) serving spammy pages, text or links, 2) phishing, 3) distributing malware. If you have a phishing notification, please do not delete this message until you have completed the entire recovery process.
4. Navigate to **Security Issues** in Webmaster tools.
   - Sites affected with malware will show a top-level heading of "Malware," and then categories of malware types, such as "Modified server configuration" or "Error template injection." In these cases, the hacker may be using your site to infect your visitors with software designed to access confidential information or harm their computers. To find out how to fix this, please continue to Assess malware damage.
   - Sites that were hacked to serve spam may display a top-level heading of "Hacked" and then categories hack types, such as "Content injection." It’s likely the hacker has placed spammy pages, text, or links on your site. To find out how to fix this, please continue to Assess spam damage.
   - Sites with a "phishing notification" in Search Console Message Center may not show any information within Security Issues. By creating phishing pages on your site, the hacker is using your site to obtain users' login, password, or financial details, often by masquerading as a trustworthy site. Since the cleanup for phishing is similar to spam, please continue to Assess spam damage.

□□□ #2
□ □□□ □□□ 2026-10-31 23:15:09 UTC
□ □□□ □□□ 2026-10-31 23:15:11 UTC