Quarantine your site

You'll need

- Ability to prevent your webserver from serving pages (alternatively, you can discuss options with your hoster). Please be aware that in later steps you'll need to bring your site backonline for short periods of time.
- Account management permissions (the ability to view all users, delete users, and change all passwords related to your account).

Next actions

1. Take your site offline

Take your site offline so that it no longer serves content to users. For example, stop your webserver or point your website's DNS entries to a static page on a different server that uses a 503 HTTP response code.

By taking your compromised site completely offline, you can complete administrative tasks with less interference from the hacker, and meanwhile, malicious code or spammy files won't be exposed to visitors. It's unlikely that taking your site offline intermittently/temporarily during the recovery process will affect future ranking of your site in search results.

- Contacting your hoster is helpful if you're unsure how to take your site offline. For instance, your hoster might configure at 503 response for your site *from outside your infected directories* (which is a fine option). Convey to your hoster that you'll soon need to toggle your site between online and offline for testing purposes as that may help them give you the most self-service method for taking your site offline.

- Having your site return a 4xx or 5xx HTTP status code isn't enough to protect your users. Harmful content can still be returned to users with 404, 503, etc. *The 503 status code is a useful signal that your site is down temporarily, but the response should occur from outside your compromised server/site.*
- Using a `robots.txt disallow` is also insufficient because it only blocks search engine crawlers. Regular users can still access harmful content.

2. Contact your hoster

If you haven't already done so, **contact your hoster to make them aware of the situation**. If your hoster was also compromised, it may help them understand the scope of the problem.

3. Perform thorough user account management

- View a list of your site's users accounts and check if the hacker created a new user account. If illicit accounts were created, write down the unwanted account names for later investigation. Then delete the accounts to prevent future logins by the hacker.
- Change the passwords for all site users and accounts. This includes logins for FTP, database access, system administrators, and content management system (CMS) accounts.

Previous
← Build a support team

Next
Use Search Console →

Last updated December 22, 2017.