

WHAT TO DO WHEN YOUR WEBSITE GETS HACKED





More than [30,000 websites are hacked daily](#), and for most business owners, finding that your website has been hacked can even be traumatic.

After all, it is the lifeblood of your business, and you want to take every possible measure to protect it.

While some people consider giving up altogether, take the following steps to recover your hacked website.

How Do Websites Get Hacked?

Hackers use a variety of methods to gain access to a website. Hackers gain access to websites in three of the following ways;

1. Access control
2. Third-party integrations
3. Software vulnerabilities

1. Access Control

The most common way hackers gain access to a website is by exploiting an account with weak access credentials. In this case, hackers can guess your login credentials and gain access to your administrative backend.

Other ways that hackers can gain access to a website include brute force attacks, Cross-site scripting, social engineering, keylogging, etc.

2. Third-Party Integrations

Third-party integrations are a common way hackers gain access to your website. These external services can include email, social media, analytics, and more.

3. Software Vulnerabilities

The most difficult type of hack is when the hacker exploits a software vulnerability to break into the site. This requires extensive knowledge about coding or the site's software to exploit the vulnerability.

In this case, a hacker will try to find poorly designed code within the website and use it against you.

What to Do When a Website Gets Hacked

Situational Awareness

After discovering that your website has been hacked, you first need to understand the circumstances that led to the breach. This means looking through log files, checking with your hosting company or other third-party partners, and taking stock of what the hacker did.

The most important thing to look for is where on your site the hack occurred: Was it a weakness in security you missed? Did they gain control by exploiting an open hole in WordPress or another CMS? If so, this will help guide which step to take next.

Inform your Web Hosting Company

It's necessary that you get in touch with your web hosting company as they can easily fix most hacking incidences by checking for and removing any vulnerabilities and malware and restoring the website from a backup.

Put Your Website in Maintenance Mode

Since your website represents your business, you need to protect all incoming traffic from accessing your hacked website.

Put the website into maintenance mode and inform your customers that you're still working on the problem.

This will prevent any accidental clicks from infecting their computer or causing other problems with malicious scripts.

It also prevents hackers from viewing private information such as customer credit card details, passwords, and bank account numbers.

Once in maintenance mode:

1. Make sure all third-party scripts and services are shut down, including analytics programs.
2. Disable logins by changing the MySQL database password (or disabling MySQL altogether).

- 3 Change your website's URL to "hacked." This is an easy step that can be done quickly.
- 4 Remove any existing content on the page, so it only displays a message to visitors.

Learn more on [how to put a WordPress website in maintenance mode](#)

Assess the File Damage Caused

Assess the extent of damage that an attacker may have caused after hacking your website.

Check your server logs, access logs, and error logs. Also, compare the most recent backup to the deleted site to understand the scope of the damage.

Some hosts offer pre-made backup images that can be downloaded and installed quickly; others may require tinkering with FTP or other software. If this is your case, make sure to ask for assistance before proceeding so as not to damage anything further!

Change Your Login Details

Someone who has hacked your website will have access to everything on it. Changing your login credentials can help you regain control over your website and prevent more problems.



This includes FTP and cPanel passwords, as well as any other password-protected areas of your site you may use. Take care not to share these new codes with anyone!

Restore a Backup of Your Website

Once you have changed all your login details, it is time to restore a backup of the hacked website. Restoring a backup is necessary in case attackers may have damaged or deleted some of your files.

If you didn't have a backup before the hack, ensure that you create regular backups of your website moving forward.

Beef up Your Website Security

It is likely that restoring a backup of your website will not fully resolve the problem, as hackers may have managed to do some damage.

In this case, you should beef up your site's security by updating any plugins or extensions they used to infiltrate.

Use firewalls or other tools to block any IP addresses that may be attacking your site.

You should also scan the website and computer for malware or viruses using antivirus software and install website security software such as Wordfence Security Plugin to protect your website from malware infections

References

<https://www.siteguarding.com/en/what-to-do-if-your-website-has-been-hacked>

<https://sucuri.net/guides/how-to-clean-a-hacked-website/>

<https://blog.sucuri.net/2021/03/how-do-websites-get-hacked.html>