

Website SOS guide – Hostinger Learning lab

CONTENTS

What's inside

01	What to do when your website acts up?	p.03
02	My site is slow	p.03
03	My site is down	p.04
04	My site may have been hacked	p.05

What to do when your website acts up?

Whether your site has slowed to a crawl, gone completely offline, or been compromised, you need answers fast. Scroll down to your issue and follow the suggested steps.

My site is slow

Pages are loading, but taking too long.

1 Run a speed test

Use Google PageSpeed Insights or GTmetrix to get a score and see exactly what's slowing things down. Note the specific issues it flags before doing anything else.

2 Compress your images

Oversized images are the most common culprit. Aim for under 200 KB per image. Use WebP format where possible — it's smaller than JPEG or PNG without visible quality loss. Tools like Squoosh or ShortPixel can do this quickly.

3 Enable caching

Caching stores a version of your pages so they load faster for returning visitors. On WordPress, install a caching plugin like WP Rocket or W3 Total Cache. Many hosts offer server-level caching you can switch on from your control panel.

4 Minify CSS, HTML, and JavaScript

Minification strips out unnecessary characters from your code files to make them smaller. On WordPress, most caching plugins handle this. If you're on a website builder, check your settings — many do this automatically.

5 Deactivate plugins and extensions one by one

Too many plugins — or a single poorly coded one — can drag down your speed significantly. Deactivate them one at a time and re-run your speed test after each to find the offender.



****Still slow after all of this?**** Your hosting plan may be underpowered for your traffic. Consider upgrading to a higher-tier plan or switching to managed WordPress hosting with built-in performance tools.

My site is down

The site isn't loading at all or showing an error.

1 Check if it's down for everyone

Visit downforeveryoneorjustme.com and enter your URL. If it's only down for you, the problem is local – try a different device or network. If it's down for everyone, keep going.

2 Check your hosting provider's status page

Look up your host's status page or social media for any reported outages. If there's a known server issue on their end, all you can do is wait and monitor – it's out of your hands.

3 Read the error message carefully

The error code tells you a lot. A 500 error is a server-side problem. A 404 means the page doesn't exist. A 503 means the server is overloaded or down. Search the specific error code for targeted fixes.

4 Trace back any recent changes

Think about what changed right before the site went down. A plugin update, a theme edit, a new piece of code? Undo that change and see if the site comes back. If you're on WordPress, put it in recovery mode from the login screen.

5 Restore from a backup

If you can't find the cause, restore the most recent backup from before the problem started. This should get the site live again while you investigate the root cause separately.



****Still down and no backup available?**** Contact your hosting provider's support team directly. Have your domain name, account details, and a description of the error ready before you reach out.

My site may have been hacked

You've noticed strange content, redirects, or a security warning.

1 Put the site into maintenance mode immediately

Stop visitors landing on a compromised site while you investigate. Use a maintenance mode plugin or contact your host to temporarily suspend the site.

2 Run a malware scan

Use a tool like Sucuri SiteCheck or your host's built-in scanner to scan for malware, injected code, and blacklisting. This will tell you what's been compromised and how serious it is.

3 Change all passwords immediately

Reset your WordPress admin password, hosting control panel password, FTP credentials, and any connected email accounts. Use strong, unique passwords for each one.

4 Restore from a clean backup

Restore a backup from before the attack. Once restored, immediately update WordPress core, all themes, and all plugins – outdated software is the most common entry point for attackers.

5 Harden your site going forward

Enable two-factor authentication on your admin account, install a security plugin (like Wordfence or iThemes Security), delete any unused themes and plugins, and make sure automatic backups are switched on.



****Can't clean the site yourself?**** Contact your hosting provider — many offer malware removal as part of their support. You can also use a specialist service like Sucuri's site cleanup, which handles the full removal for you.

Prevent the next problem before it happens

Most of the issues in this guide are preventable with the right hosting setup. Hostinger plans include automatic daily backups, built-in security tools, and 24/7 support – so if something does go wrong, you're not dealing with it alone.

[Get started →](#)