THE HACK REMOVER

WORDPRESS SECURITY

The ten-point security check *for a* small business site

Most hacked WordPress sites are not targeted. They are found. Automated scanners sweep the web looking for software nobody updated, so the work below is less about defence and more about closing what is already open.

01 **Update everything, this week**

Core, plugins and themes. An available patch you have not installed is the single most common way in.

02 **Delete what you do not use**

Deactivating is not removing. Fewer installed components means fewer things to keep patched.

03 **Two-factor on every admin login**

A stolen password should not be enough on its own to reach your dashboard.

04 **Unique passwords, kept in a manager**

Reuse turns one breach somewhere else into a breach of your site.

05 **Count your administrators**

Know who holds admin access and why. Remove accounts that belong to former staff or past developers.

06 **Back up away from your host**

A copy stored inside the same hosting account leaves with the site. Test that you can actually restore it.

07 **Connect Google Search Console**

It is how you find out that you have been flagged, and how you ask for the flag to be lifted.

08 **Know your hosting, DNS and domain logins**

Recovery starts with access. If only someone else has it, the clock is already running.

09 **Revoke access you no longer need**

Old developer logins, FTP accounts and API keys outlive the projects they were made for.

10 **Decide who you call before you need to**

Writing down the host, a security contact and an insurance number is free, and it saves hours.

SIGNS YOU ARE ALREADY IN IT

- ☐ An administrator you did not create
- ☐ A warning in Google results or the browser
- ☐ Customers receiving strange email from you
- ☐ Visitors sent somewhere you did not set
- ☐ Spam pages or links under your domain
- ☐ Your host notices before you do

The Hack Remover · website cleanup, hardening and recovery support
hackremover.com/blog · info@hackremover.com