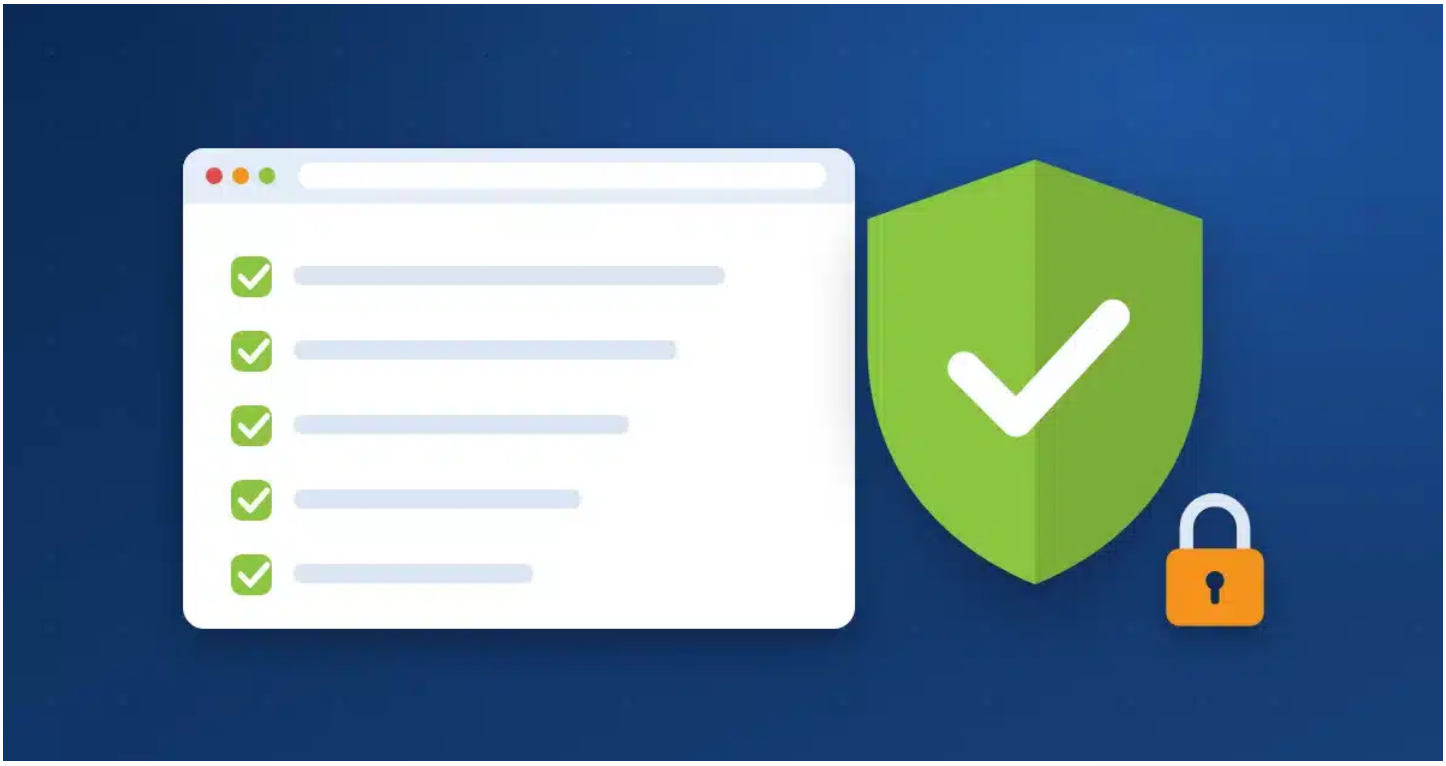
How to Protect Your Website from Hacking: 10 Practical Steps

Website Security · https://www.hyyat.com/en/knowledgebase/protect-website-from-hacking/

In short Most websites are hacked through a known flaw in an outdated plugin or theme, or through a weak or reused password. Protect your site with long unique passwords, two-factor authentication, regular updates to WordPress and plugins, removing what you do not use, an SSL certificate and regular backups. We protect the server itself with a firewall and daily file scans.



Website security is shared: we protect the server and the network, and you protect what lives inside your site, such as passwords, plugins and user permissions. This guide covers why sites get hacked, 10 practical steps you can apply yourself, and what we do on our side.

Why do websites get hacked?

1 **Outdated plugins and themes** The most common cause. Flaws in old versions are public, and attackers exploit them automatically.

2 **Weak or reused passwords** A short password is guessed by brute force, and a reused one leaks from another site and gets tried on yours.

3 **Nulled themes and plugins** Free copies of paid themes often hide malicious code that opens a backdoor into your site.

4 **Too many permissions** Every extra admin account, or an old account of someone who left, is another door that can be opened.

10 practical steps to protect your website

1. **Long, unique passwords:** Use at least 15 characters and a different password for each account: WordPress, cPanel, email and the client area. A password manager remembers them for you.
2. **Two-factor authentication:** Turn it on in your cPanel account and the client area, and in WordPress with a trusted plugin. Even a leaked password is not enough without the code.
3. **Keep everything updated:** WordPress, plugins, themes and the PHP version. WP Toolkit in cPanel offers automatic updates and vulnerability checks.
4. **Delete what you do not use:** A deactivated plugin still has its files on the server and can be exploited. Remove unused plugins, themes and test sites.
5. **Never use nulled copies:** Download themes and plugins only from the official WordPress directory or the developer’s own site.
6. **Enable SSL and use https:** Encryption protects passwords and visitor data from eavesdropping. Read what an SSL certificate is and how it works.
7. **Add a trusted security plugin:** It limits login attempts and watches for file changes. See the best WordPress security plugins.
8. **Keep offsite backups:** If your site is hacked, a backup is the fastest way back. Read why backups matter.
9. **Least privilege:** Give each user only the role they need (editor or author instead of administrator), and delete old accounts right away.
10. **Monitor your site:** Scan your files with ImunifyAV, and watch for a new admin user or strange PHP files inside the uploads folder.

Think your site is hacked? Do not delete files at random. Follow the steps to remove malware from a WordPress site, or open a ticket and we will help.

How Hyyat Host protects your site

- The **CSF firewall** blocks attacking addresses, and **cPHulk** stops password guessing. Read brute force protection.
- **Imunify360** and **ModSecurity** rules stop known web attacks before they reach your site. Read managing ModSecurity.
- **ImunifyAV** scans files daily for malware.
- **CloudLinux** isolates every account, so another site on the same server cannot affect yours.
- A **free SSL certificate** is issued automatically on most plans, and you can connect your site to Cloudflare.

On a VPS or dedicated server, securing the server itself is your responsibility, and we can handle it for you with our server management service.

Frequently asked questions

Is secure hosting enough to protect my site?
No. Hosting protects the server and the network, but an outdated plugin or a weak password inside your site is still your responsibility. Security works when both sides do their part.

How often should I update WordPress and plugins?
As soon as security updates are released, and review your site at least weekly. You can turn on automatic updates in WP Toolkit in cPanel.

Do I need a security plugin if the hosting is protected?
It is recommended, because a plugin protects the login page and watches your site’s files from the inside, which complements server protection.

Related guides

- Brute Force Protection: What It Is and How Hyyat Host Protects Your Site
- How to Protect Your Customers’ Data on Your Website: A Practical Guide
- Hacking Tools: C99 Shell

- What Is an SSL Certificate and How Does It Work?

All website security guides →

Need this service from Hyyat Host?Our team handles it for you, with support replying to tickets within 24 hours at most.

Web HostingSaudi Hosting