

VIEWEN



ULTIMATE WORDPRESS & CPANEL SECURITY GUIDE

Viewen.com Security Promise: Our hosting infrastructure is built on trust and fortified with enterprise-grade security. We deploy advanced RSA encryption and Let's Encrypt automated SSL. **Crucially, if any hacker attempts unauthorized access or brute-force logins to your cPanel, our automated firewall bans their IP address instantly.** We neutralize threats at the server level before they reach your site.

However, securing a website is a shared responsibility. While the Viewen server environment is locked down, individual WordPress websites can still be compromised through the application level—most commonly via outdated plugins, weak credentials, or theme vulnerabilities.

1. SSL Encryption vs. Application Security

A frequent misconception is that an SSL certificate alone prevents a website from being hacked. Here is the distinction:

- **SSL/TLS Encryption:** Secures the connection between a visitor's browser and the server. It prevents attackers from intercepting passwords or sensitive data in transit, but it does not stop a hacker from interacting with your website.
- **Application Security:** Protects your actual WordPress files, plugins, and database. Hackers often exploit hidden backdoors in poorly coded or outdated plugins to inject malware.

2. Enforcing HTTPS Connections

If your website displays an error like *"The site doesn't support a secure connection,"* it usually means your website configuration is not forcing traffic over the secure HTTPS protocol.

Method A: The .htaccess Method (Recommended)

You can force all traffic to use SSL by adding a rewrite rule to your `.htaccess` file located in your `public_html` directory:

```
RewriteEngine On
RewriteCond %{HTTPS} !=on
RewriteRule ^.*$ https://%{SERVER_NAME}%{REQUEST_URI} [R,L]
```

Method B: The Plugin Method

If you prefer a simpler route, install the **"Really Simple SSL"** plugin from the WordPress repository. Once activated, follow the prompts to configure your site to strictly use the HTTPS protocol.

3. Securing WordPress with Wordfence

Because the majority of compromises occur via outdated plugins, deploying a Web Application Firewall (WAF) is essential. We strongly recommend configuring **Wordfence Security**.

- **Install and Activate:** Search for "Wordfence Security" in your WordPress plugin directory and install it.
- **Optimize the Firewall (WAF):** In the Wordfence dashboard, click "Optimize the Wordfence Firewall." This ensures the firewall loads before WordPress does, blocking malicious requests early.
- **Enable 2FA (Two-Factor Authentication):** Navigate to Login Security within Wordfence. Activate 2FA for all Administrator accounts to eliminate the risk of brute-force password guessing.
- **Automated Scans:** Configure scheduled Standard Scans to continuously monitor for core file changes, malicious code, and known plugin vulnerabilities.

4. Proactive WordPress Hardening Checklist

Security Area	Best Practice Action
Plugin Maintenance	Always keep plugins updated to their latest versions. Delete (do not just deactivate) unused themes and plugins.
Admin Accounts	Never use "admin" or your domain name as a username. Use a password manager to generate 16+ character complex passwords.
File Editing	Disable theme and plugin file editing via the WP dashboard by adding `define('DISALLOW_FILE_EDIT', true);` to `wp-config.php`.

5. Checking for Known Vulnerabilities

Before installing new plugins, or if you suspect a compromise, check reputable security databases to see if the plugins you use have unpatched security flaws:

- **Wordfence Threat Intelligence Database** always use WordFence
- **SentinelOne Vulnerability Database**

Conclusion: With Viewen's strict server-side protection instantly banning malicious IPs, combined with proactive WordPress hardening via Wordfence, your online presence is highly secure. Stay updated, enforce complex passwords, and let our infrastructure handle the rest.
