



Security Tips for Your Very Website



Wednesday, April 24, 2024

The author of the following page

<https://dev.bestwebsoft.com/blog/security-tips-for-your-very-website/> is
Anastasia.



Why Website Security is Important?



A hacked WordPress site can cause serious damage to your business revenue and reputation.



Hackers can steal user info, install malicious software, and can distribute malware to your users.



Worse, you may find yourself paying ransomware to hackers just to regain access to your website.

More than **50 million website** users have been warned about a website they're visiting may contain malware or steal information.

— Google, March 2016



Furthermore, Google blacklists around **20,000 websites** for malware and around **50,000** for phishing each week.

— Google, March 2016



Basics of WordPress Security



Keeping WordPress Updated
WordPress automatically installs minor updates. For major releases, you need to manually initiate the update.



Password and User Permission
You can make that difficult by using stronger passwords that are unique for your website.



The Role of Web Hosting
A good shared hosting provider take the extra measures to protect their servers against common threats.

WordPress Security in Easy Steps



1
Install a WordPress Backup Solution



2
Best WordPress Security Plugin



3
Enable Web Application Firewall

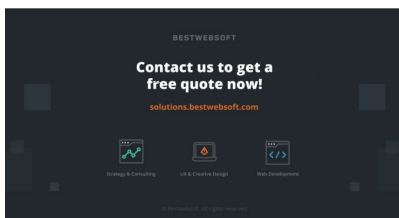


4
Move WordPress Site to SSL/HTTPS

WordPress Security for DIY Users

If you do everything that we have mentioned thus far, then you're in a pretty good shape. But as always, there's more that you can do to harden your WordPress security. Some of these steps may require coding knowledge.

- Change the Default "admin" username**
There are three methods you can use to change the username. Create a new admin username and delete the old one. Use the Username Changer plugin Update username from phillyAdmin
- Disable File Editing**
You can easily do this by adding the following code in your wp-config.php file. Alternatively, you can do this with 1-click using the Hardening feature in the free Sucuri plugin that we mentioned above.
- Disable PHP File Execution**
Can do this by disabling PHP file execution in directories where it's not needed such as /wp-content/uploads/. Also, you can do this with using the Hardening feature in the free Sucuri plugin that we mentioned above.
- Limit Login Attempts**
You can use Limit Attempts, a plugin from Bestwebsoft that protects your WordPress site from brute force attacks.
- Limit Attempts**
4.5 ★
10k+ active installs
- Add Two Factor Authentication**
This technique requires users to log in by using a two-step authentication method. The first one is the username and password, and the second step - authenticate using a separate device or app.
- Fixing a Hacked WordPress Site**
Allow a professional security company like Bestwebsoft to fix your website will ensure that your site is safe to use again. It will also protect you against any future attacks.
- Disable Directory Indexing and Browsing**
You need to connect to your website using FTP or cPanel's file manager and locate the .htaccess file in your website's root directory. After that, you need to add the following line at the end of the .htaccess file: Options-Indexes
- Disable XML-RPC in WordPress**
There are 3 ways to disable XML-RPC in WordPress, and we have covered all of them in our step by step tutorial. If you're using the web-application firewall mentioned earlier, then this can be taken care of by the firewall.
- Automatically logout idle Users**
You will need to install and activate the Inactive Logout plugin. Upon activation, visit Settings > Inactive Logout page to configure plugin settings.
- Add Security Questions to Login**
You can add security questions by installing the WP Security Questions plugin. Upon activation, you need to visit Settings > Security Questions page to configure the plugin settings.
- Scanning WordPress for Vulnerabilities**
You can use your WordPress security plugin, or use one of these malware and security scanners.
- Change WordPress Database Prefix**
You can add additional password protection on a server-side level, which will effectively block those requests. This allows to try their hacking tricks or run DDoS attacks.
- Password Protect WP-Admin and Login**
You can add additional password protection on a server-side level, which will effectively block those requests.



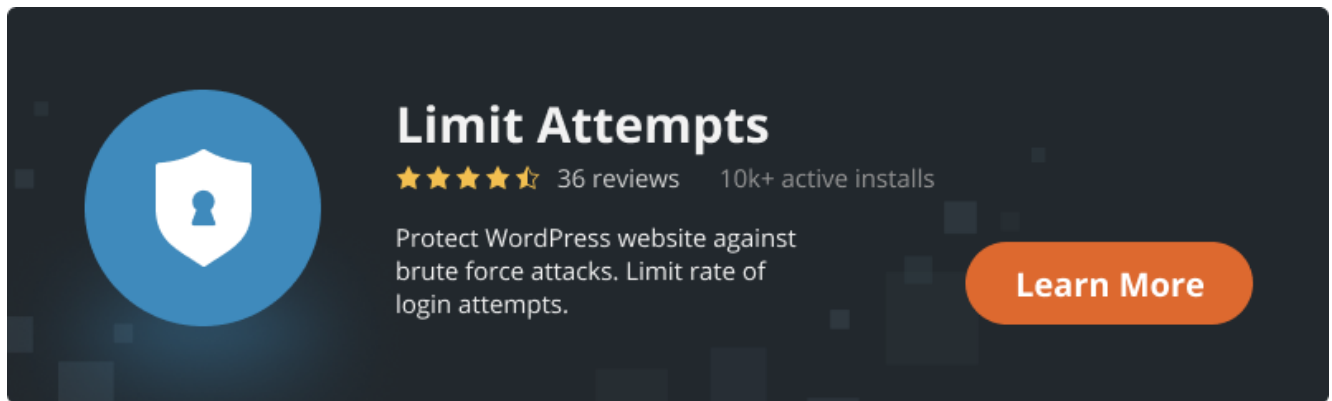
Wednesday, April 24, 2024

The author of the following page

<https://dev.bestwebsoft.com/blog/security-tips-for-your-very-website/> is Anastasia.



Want more powerful protection for the website? Use the Limit Attempts by BestWebSoft plugin to set the number of failed user attempts to protect the website from brute-force attacks and much more.



Limit Attempts
★★★★☆ 36 reviews 10k+ active installs

Protect WordPress website against brute force attacks. Limit rate of login attempts.

[Learn More](#)

Wednesday, April 24, 2024

The author of the following page

<https://dev.bestwebsoft.com/blog/security-tips-for-your-very-website/> is
Anastasia.