WPHackedHelp Blog
GET IT FIXED FAST!

HOMEPAGE › WORDPRESS SECURITY

Wordpress Security

WordPress Security Checklist Guide 2024 – [UPDATED]

Table of Contents [TOC]

WordPress security is the same as home security. When you leave your home or office, you close the doors, windows and all open access you see, right? Why wouldn’t you do the same with your website?

The security of a WordPress site is not to be taken lightly in 2024. WordPress can be hacked anytime, so you must take preventive actions by Implementing these WordPress Security tips 2024 to Secure Your WordPress Site from various WordPress Security vulnerabilities .

Hackers do not attack all WordPress sites. They only target vulnerable WordPress sites, ones that are easy to hack. If your WordPress site is properly secured, it wont be easy for a hacker to find the tiny security hole that would give him access to your server and hack wordpress site.

Understanding why your WordPress website needs a solid security plan can help you put the appropriate proactive security measures in place, stopping hackers and malicious software from breaching your system.

At WP hacked help, we understand how important it is to secure your WordPress website. That is why our team has put together this ? WordPress Security Guide Checklist that includes various helpful tips for securing your WordPress site. This will also act as a step by step WordPress security guide for all WordPress Security Issues. We have included an **Infographic** as well as

WordPress security guide PDF for you to download.

In this Updated WordPress Security Checklist, you will learn, how to keep our WordPress website safe as per WordPress Security Implementation Guidelines from OWASP. You should bookmark this page for future reference. This is a very detailed post (and therefore long) that will help you in doing full Security audit of WordPress site. So have a cup of coffee and let's start.

Also Read – ?How to secure your WordPress site from hackers[Updated]

Tools You Need – Online WordPress Security Scanners To find Vulnerabilities

⚡ WordPress Security Plan

It is important to note that WordPress is one of the most commonly hacked content management systems (CMS) on the Internet. Therefore every security plan starts with a thorough in-depth scan of your site. Luckily, we got you covered, lets find out if your site is secure or not.

› Run A WordPress Security Scan Now

Taking your WordPress website security seriously by implementing a WordPress security plan in 2020 can help protect your website from hackers and other malicious attacks.

It is important to implement a ? WordPress security checklist that is constantly evolving, ensuring regular updates along with this WordPress maintenance checklist.

Looking for an easy WordPress

Looking for an easy WordPress security checklist to harden security of your WordPress site? Look no further. We already use it for helping clients.

Make your installation more secure than your neighbor 🙂

⚡20 Point WordPress Security Checklist 2024

[A Step By Step Guide To Secure Your Website]

DOWNLOAD DOC – PDF 1 – PDF 2

You can also download our wordpress security guide from – Open.edu Open Couses

---

WP-CONFIG.PHP

Configure the WordPress security keys?

Protect your WP-login

Use WPS Hide Login plugin
Login LockDown plugin to Stop Hackers
Enable Two-factor Authentication (2FA)
Rename the URL of your WordPress Login Page
Use an email address instead of username
Remove visible login links from the theme

Create a strong password

Change your WordPress credentials regularly

Generic error message for an incorrect username or password

Disabling the REST API on WordPress

Protect Your WordPress Admin

Create a password protected directory

Keep your WordPress up-to-date

Remove admin account and creating a new account

Create user roles on WordPress

Use SSL on your WordPress site

Install WordPress security plugins

Scan the website for viruses, malware, and security breaches

WordPress Theme Security

Update WordPress plugins

Secure WordPress Database

Change the prefix in the database

Schedule daily Backup of the WordPress database

Use Secure WordPress Hosting

Features To look for in a Web Hosting Provider

WORDPRESS SECURITY CHECKLIST

CHECKLIST

LOGIN PAGE(9)

✔ Lockdown the login page for repetitive failed login
✔ Activate 2 factor authentication (Google Authentication)
✔ Use email address to login instead of username
✔ Rename the URL of your login page
✔ Remove login links from the theme
✔ Use a strong password
✔ Change the passwords regularly
✔ Make the login error messages more generical
✔ Disable the WP REST API, if you aren't using it.)

ADMINISTRATIVE PANEL(7)

✔ Password protect the folder wp-admin
✔ Keep WordPress up-to-date
✔ Do not create an account with username admin.
✔ Create an Editor account and use it solely to publish content
✔ Implement SSL for the WordPress admin section
✔ Install any plugins to check file changes
✔ Scan the website for malware - Use WPHackedHelp Scanner

THEMES(4)

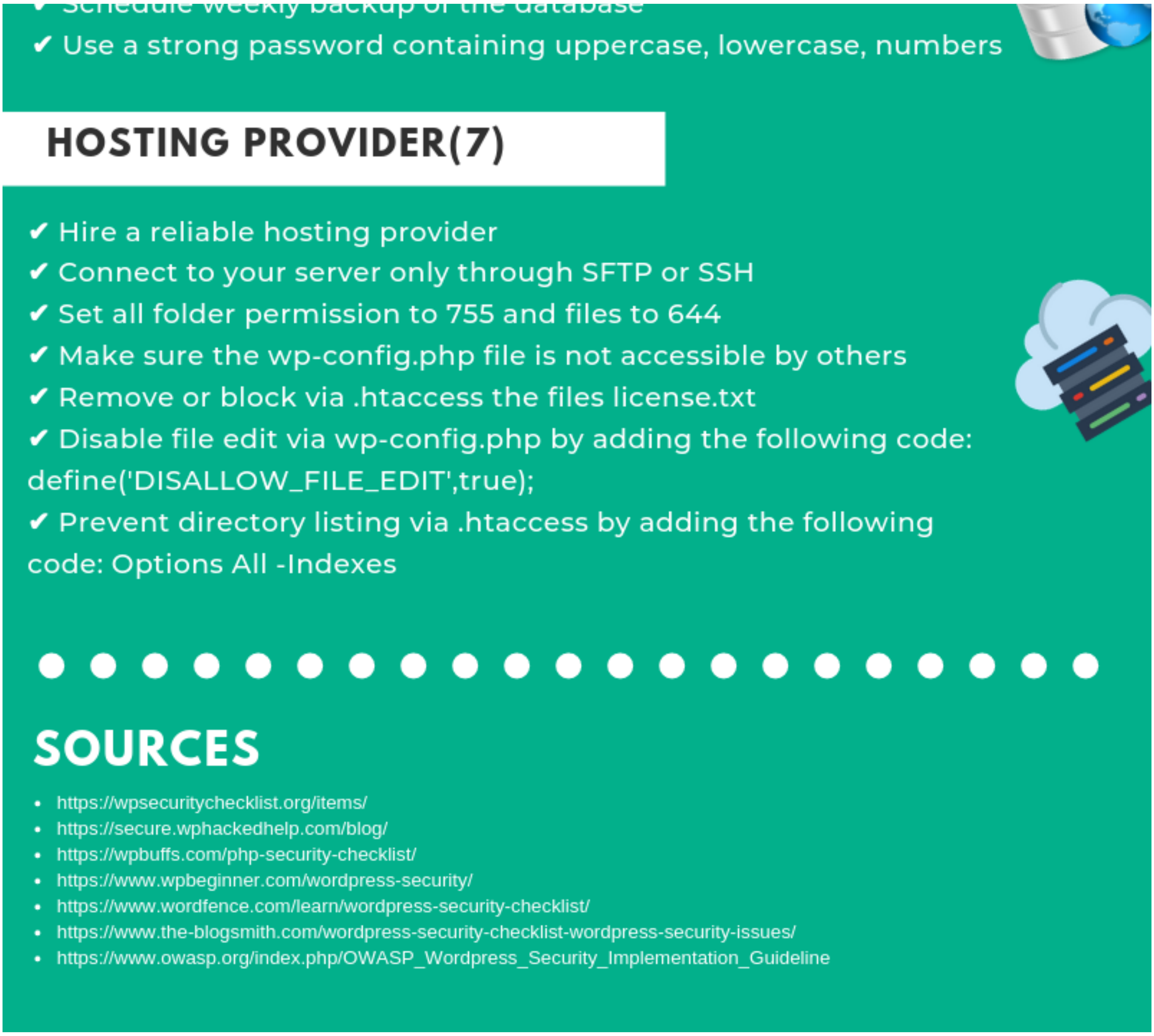
✔ Keep the theme up-to-date
✔ Delete and remove unused themes
✔ Download and use themes only from reputable sources
✔ Remove the WordPress version from the theme

PLUGINS(5)

✔ Keep all plugins up-to-date
✔ Delete and remove unused plugins
✔ Download and use plugins only from reputable sources
✔ Replace outdated plugins for alternative newer plugins
✔ Think twice before installing a ton of plugins

DATABASE(3)

✔ Change the default table prefix
✔ Schedule weekly backup of the database



✔ Schedule weekly backup of the database
✔ Use a strong password containing uppercase, lowercase, numbers

HOSTING PROVIDER(7)

✔ Hire a reliable hosting provider
✔ Connect to your server only through SFTP or SSH
✔ Set all folder permission to 755 and files to 644
✔ Make sure the wp-config.php file is not accessible by others
✔ Remove or block via .htaccess the files license.txt
✔ Disable file edit via wp-config.php by adding the following code: define('DISALLOW_FILE_EDIT',true);
✔ Prevent directory listing via .htaccess by adding the following code: Options All -Indexes

SOURCES

- https://wpsecuritychecklist.org/items/
- https://secure.wphackedhelp.com/blog/
- https://wpbuffs.com/php-security-checklist/
- https://www.wpbeginner.com/wordpress-security/
- https://www.wordfence.com/learn/wordpress-security-checklist/
- https://www.the-blogsmith.com/wordpress-security-checklist-wordpress-security-issues/
- https://www.owasp.org/index.php/OWASP_Wordpress_Security_Implementation_Guideline

WP-CONFIG.PHP

A configuration error of a website can be catastrophic for its security. However, the configuration of a WordPress site is defined in the file wp-config.php.

The connection parameters to the database, security keys are all information contained in the file wp-config.php that would allow an attacker to take control of the site. Fortunately, a few precautions can protect access to the wp-config.php file while some instructions added in wp-config.php can improve the security of the site.

Configure WordPress security keys

To configure the security keys in the wp-config.php file, follow the procedure below:

Open the wp-config.php file

Search Unique Keys for Authentication and Salts. This section should be right after the database credentials unless you have moved this information to your wp-config.php file.

Specify a random value of more than 60 unique characters for each key and for salting instead of putting your unique phrase here. You can also use the Online Security Key Generator for automatic key generation.

If you are using the online security key generator, simply copy the entire block of code and replace the eight default values in your wp-config.php file.

Save the wp-config.php file.

Change the security keys & salts with a plugin

If you want to change the security keys periodically, a wordpress security keys generator plugin like Salt Shaker could help you in the process of changing these keys.

After installing the plugin, you will see that it can be configured from Tools> Salt Shaker page in your WordPress dashboard to configure your plugin.

Other Generators Are:

- Secret Key Generator for WordPress by MD5.me
- WordPress Secret Key Generator

Web Application Firewall (WAF)

A website firewall blocks all malicious traffic before it even reaches your website. It can be installed on any server with PHP, Apache, or Nginx installed.

PHP WAF

The most common type of WAF that you'll find on WordPress installations is a PHP application firewall (or PFW). These use rules based on the HTTP headers and client IP address to block requests that are deemed malicious in nature.

DNS Level Website Firewall –

A DNS level firewall is designed to detect and block suspicious traffic at the DNS layer (Domain Name System) of your domain name server (DNS) server. This type of firewall is designed to protect an entire domain, not individual websites or applications. A DNS level firewall will scan for known bad IP addresses and block them from accessing your site.

Application Level Firewall –

An application level firewall protects an individual application (or set of applications) from threats that have been detected at the network layer (Internet Protocol). Application level firewalls can be used on either a single computer or multiple computers that share resources such as files, printers and databases.

Protect your WordPress login

A WordPress website usually has many chances to deal with brute force attack on wordpress and malicious connection attempts. There are several ways to solve this problem in which the best is to deploy multiple policies. So, in this case, we will provide you the best way to get rid of this problem and hide your WordPress login page.

Use WPS Hide Login plugin

With the help of this plugin, you can use a custom URL as a standard login URL. After the installation and activation of the plugin, "/wp-admin" and "/wp-login.php" will be inaccessible and will be replaced by a custom URL that you have chosen.

Also Read – How To Change Your WordPress Username? – 3 Easy Ways

Login LockDown plugin to Stop Hackers

For example, after 5 unsuccessful attempts, you are entitled to think that the user trying to log in is not allowed. In this case, it is necessary, at least temporarily, to lock access to the login page for this user. Now, this is possible with the help of the Login LockDown plugin.

Enable Two-factor Authentication (2FA)

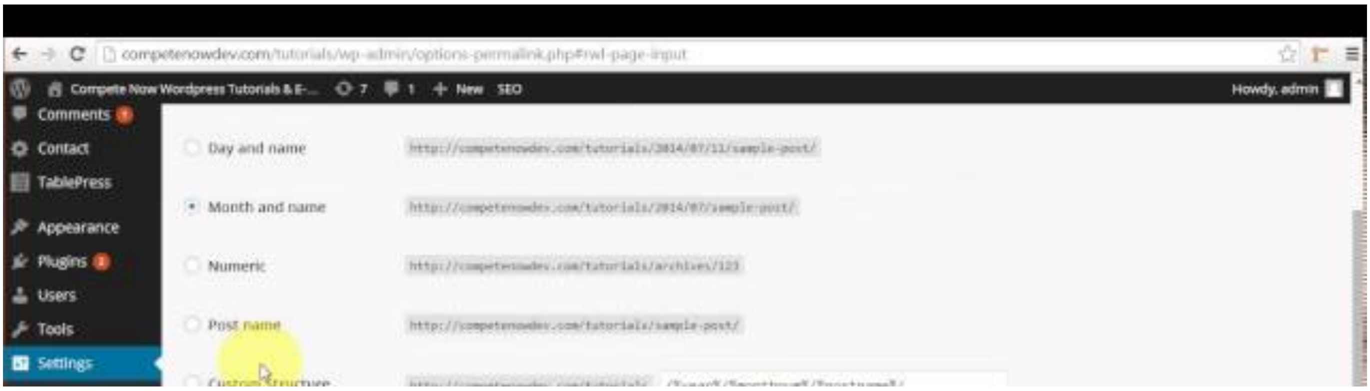
It is very important to setup/enable WordPress Two-factor Authentication, because in case of password theft (via Man-in-the-middle attacks, phishing or other), there is no barrier anymore for the criminals who want to connect to one of your accounts.

And this can have dramatic consequences such as the theft of money (PayPal, the bank, etc.), Or identity theft (Twitter, Facebook, your mailbox, etc.)

The sending of code by SMS or email is the most common and convenient method. All you have to do is to have your mailbox or SIM card with the correct phone number and it is set.

Rename the URL of your WordPress Login Page

If you too are constantly undergoing brute force attacks that target your login form to your admin area and default to url /wp-login.php or /wp-admin, then the solution is simply to change this URL.



competenowdev.com/tutorials/wp-admin/options-permalink.php#rwl-page-input

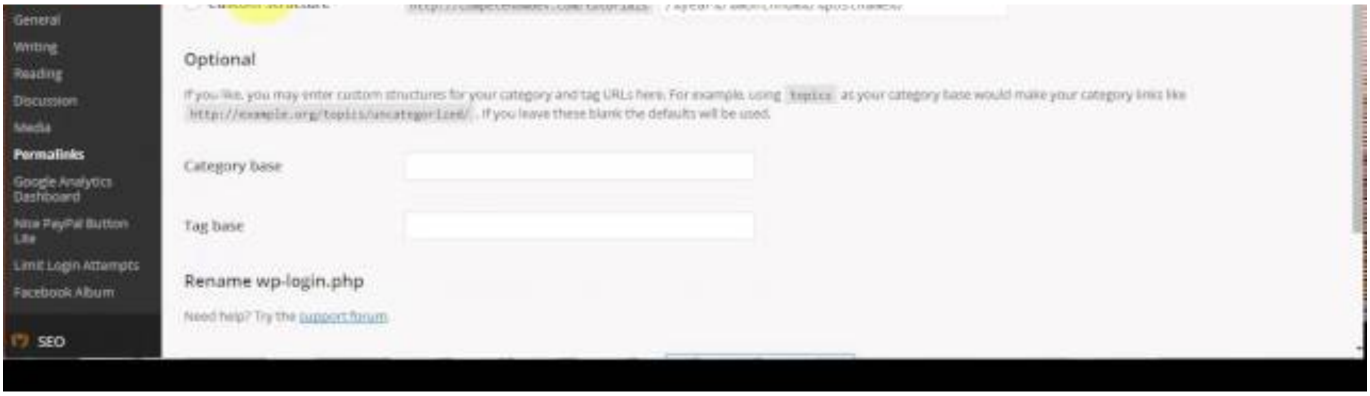
○ Day and name http://competenowdev.com/tutorials/2014/07/11/sample-post/

● Month and name http://competenowdev.com/tutorials/2014/07/sample-post/

○ Numeric http://competenowdev.com/tutorials/archives/123

○ Post name http://competenowdev.com/tutorials/sample-post/

○ Custom Structure http://competenowdev.com/tutorials



Optional

If you like, you may enter custom structures for your category and tag URLs here. For example, using `topics` as your category base would make your category links like `http://example.org/topics/uncategorized/` . If you leave these blank the defaults will be used.

Category base

Tag base

Rename wp-login.php

Need help? Try the support forum.

There are several extensions in the official plugins directory that meet this need but in different ways. Some are renaming or moving files in the kernel of the WordPress installation, others use rewrite rules with the .htaccess file.

just add this to your `.htaccess` file:

```
RewriteRule ^banana$ http://example.com/wp-login.php [NC,L]
```

Now `http://example.com/banana.php` is your login page.

Also Read – ? WordPress .htaccess hacked – Cleanup & Prevent .htaccess Attack

Use rename LOGIN.PHP plugin

Rename login.php is the plugin we are talking about and that is aptly named. The plugin is very well rated on the official page and it is really super light (82 KB), it does not risk to burden your site and it will save you bandwidth by preventing all attempts to connect to your administration space by robots that do not hesitate to go back many thousands of times by your page /login.php.

Well, let's move on to installing the plugin. Once done and activated, you will be automatically redirected to the Settings> Permalinks page to enter the name of your new URL:

Enter the name you want to give to your login page and click save. Your new login URL will then be – http://yoursite.com/new-page-connection.

Use an email address instead of username

Nobody remembers such username which contains long alphanumeric characters like that. So, this is recommended to enable login with email or at least create a feature for changing my username. To implement this successfully you can use Force Email Login plugin.

1. Email Address Only – Users can only login using their email address which disables logging in by using a username.
2. Username Only – Users can only log in using their username which disables logging in using an email address.

Remove visible login links from the theme

Remove the links like “Lost password”. It is very useful but if someone has hacked your email he will be able to have your WordPress password and take control of your site.

To remove this link, add this code to your login-style-perso.css file:

```
p#nav {

display: none;

}
```

Remove the link «Back to the site»

This link allows users to return to the homepage of the site. We choose a very clean style and therefore wants to make it disappear from the login form. Add this code to your style-login.css file:

```
p#backtoblog{

display: none;

}
```

Create a strong password

The best way to maintain an account would be to secure the password. However, you should know that there is no 100% secure password. The length of the term used as a password is very important. Eight characters may suffice, but its relevance is not assured.

The ideal would be to opt for a term making a minimum of 14 characters. This is the number of characters shown for passwords consisting only of numbers or letters. It is much more complicated to guess and hack a password consisting of different types of characters on the keyboard.

Do not hesitate to combine diacritical marks, symbols, numbers and letters, possibly with a mixture of the upper and lower case. This is the perfect formula, especially for mailing services.

Also Read – How to Password Protect A WordPress Site/Post

Use A Strong password generator

Create a secure password for your WordPress account with the help of Password Generator and LastPass. It generates a strong password including letters, numbers and symbols.

Change your WordPress credentials regularly

By default, WordPress creates an "Admin" identifier. In order to secure your site, we can only advise you to make changes to your login and create a secure password. To be really effective, a password must be longer than 8 characters and you must change your credentials regularly.

Find Additional WordPress security tips to secure your wordpress site in 2019.

Generic error message for an incorrect username or password

It is very common (a basic security type) that is displayed on the login page if the username or password was incorrect when a user tries to log in. One should show a generic message, such as "Password or username is incorrect.

Disabling the REST API on WordPress

It cannot be denied that the WP REST API will bring a lot of benefits to WordPress developers. However, some website owners may not need these features. The API makes it easy to retrieve data using GET requests. This is extremely useful for design applications on WordPress.

> *If you want to try a completely different solution you can try out https://wordpress.org/plugins/disable-json-api/ which takes care of removing the REST API functionlity for you.*

That being said, this could expose your site to a new front of WordPress DDoS

That being said, this could expose your site to a new front of WordPress DDoS attacks. It can be greedy in resources and therefore slow down your website. This is similar to disabling XML-RPC, which many site administrators disable on their WordPress sites for security.

If you want to disable the WP REST API on your WordPress site, then you can easily do it by simply adding the following code in your theme’s functions.php file or on a plugin page. Or in one of your WordPress plugins.

```
add_filter ('json_enabled', '__return_false');

add_filter ('json_jsonp_enabled', '__return_false');
```

This code simply uses built-in filters to disable the JSON and JSONP REST API.

Protect Your WordPress Admin Panel

Security is an extremely important aspect of running your online business. Some parts of your website are certainly more important than others. An

Some parts of your website are certainly more important than others. An example would be access to the administrative areas of your website where important changes can be made.

Create a password protected directory

You can create a password-protected directory from your cPanel. Look for the directory password icon and select it. Once you have done and WordPress has been installed, you should be able to find the wp-admin folder. Select the folder (wp-admin) for which you want to create a password-protected directory.

You can change the name of the chosen directory (unblock only the needed files) and enable passwordless protection in wordpress. Create a user with a username and password (make sure the password is strong), and you're done. You have password protected your wp-admin folder.

Keep your WordPress up-to-date

This will allow you to secure WordPress effectively, it seems simple, but only 22% of sites using WordPress use the latest version. Between us, who has never been lazy not to update his site? If you want to have a clean and virus-free website, it's mandatory.

WordPress has incorporated the automatic update in versions, however, it only works for small security updates. So, major updates must be done manually to secure WordPress.

Remove admin account and creating a new account

To get rid of the Admin account when a blog is powered via WP.org, it consists in short:

to create a second admin account with another login

to create the second account with all the information from the admin account (without admin of course)

to assign all items to the new account “Login”

to finish, delete the account admin

Creating a new account

Open WP dashboard, go to the Users section on the left, just under Extensions. Once here, click on > Add New to go to create a new user profile.

Also Read – How To Delete Hidden Admin User In WordPress?

Create user roles on WordPress

User roles have been integrated on WordPress since version 2.0. Most users do not even know that they exist and assign administrator rights to everyone who has access to their dashboard (obviously this is not a good thing for a lot of reasons). By default, WordPress comes with 6 user roles:

Super Administrator: The Super Administrator is one with the highest level of access to WordPress and is only available on a multi-site network. It looks like an administrator but has more power than a normal administrator.

Administrator: someone who has access to all administrative functions and

Administrator: someone who has access to all administrative functions and functions within a site.

Editor: someone who can publish and manage the articles of all users, including his own.

Author: someone who can publish and manage his own articles.

Contributor: someone who can write and manage their own messages but cannot publish them.

Subscriber: someone who can only manage his profile and read the published articles.

Also Read – How to Log User Activity in WordPress? [2024] GUIDE

Use SSL on your WordPress site

Sharing our information is so common now that we do not think twice before doing anything. This is where SSL comes in. SSL protects the details we share online, which prevents it from falling into the wrong hands.

An SSL Certificate is critical for any website in 2019. In July 2018, Google's Chrome Browser began marking non-HTTP websites as not secure. We believe that an SSL Certificate will become increasingly important in 2019. In fact, we predict that Google will fully transition into ranking HTTPS websites higher than HTTP websites in search results.

Websites that have an SSL certificate have an extra encrypted buffer between their server and all others. This means that websites that have made the transition from HTTP to HTTPS are labeled as secure and are rewarded with a higher ranking by search engines like Google.

Apart from that, if your site requires users to log in or provide personal information such as their name, address, credit card details and more, you need SSL protection. Without this, your user's information can easily be compromised.

Install WordPress security plugins

Try finding an all-in-one security WordPress plugin that will help cover all of your bases. Some of the things that you should look for in a security plugin include:

- A WP firewall
- DDoS scanner and protection
- Enabling of two-factor authentication
- Enforcement of stricter password standards
- Geography-based blacklisting
- IP blacklisting and whitelisting capabilities
- Block specific country IP addresses in wordpress
- Malware monitoring and protection
- Monitoring of database, themes, and plugins for file changes

There are many WordPress security plugins and Cleanup services for WordPress, among them:

1. WP Hacked Help allows the scanning and cleanup of your site after being hacked.
2. Google Authenticator is a WordPress plugin associated with the google authenticator application to verify the identity of the person who connects.
3. BulletProof Security protects the main weaknesses of WordPress.
4. Acunetix WP Security optimizes your WordPress installation by closing the main vulnerabilities and providing you with real-time connection tracking.
5. Finally the SecuPress.

Scan the website for viruses, malware, and security breaches

WP Hacked Help is one of the best WordPress security services which offers online wordpress malware scanning that allows you to manually run an anti-malware scan to check if your site is infected by a malware. (**Also Read** – How To Remove Malware From WordPress Site]

The tool generates a malware analysis report and a blacklisted surveillance report to search for key signs of malware, such as spamming, site disfigurement, and so on.

Following issues can be easily found during a scan alongwith removals which are taken care of in later stage.

Malware detection eg: wordpress malware redirect from one site to another

Website Hacked instances & Types of hacks attacks such as [WordPress Xss vulnerability , WordPress Pharma Hack, Backdoor hack, eval(base64_decode() hack, Japanese Keyword hack and many more.]

Google Blacklist check

- Google Warning Removals
- Prevent Future Website Hacks with the help of Virtual Hardening
- Daily Automatic Backup
- Daily, Monthly and Weekly Monitoring
- Free Backup Restores
- Backup of all WP Plugins, Images, files & Media

The scanning is free, but in case of detection of malicious code, the establishment of automatic monitoring is paid. If you discover that your site has been infected, you can choose to remove malware from wordpress yourself or, if you are not comfortable with this type of operation, you can entrust our professionals.

WordPress Theme Security

As for your CMS, your plugins and WordPress themes are gateways for attackers. And as for your CMS, there are regular updates. You will need to perform them as soon as possible.

As for modules, there are a multitude of WordPress themes. Take the time to compare the themes before choosing one. Whether free, freemium or paid, the important thing is to have a well-coded theme. Check to see if there is a support team to make updates.

You can check the technical consistency of a theme with the " Theme-Check " plugin (which will require you to install your theme before analyzing it). In any case, pay close attention to the download sources.

We advise you to download themes from reliable and recognized sites such as WordPress.org and Themeforest.

Most important do not forget to scan your overall website, this will prevent you from downloading and installing malware-infected themes.

These tips are relevant, especially to Improve WordPress theme security:

1. Keep your WordPress theme up-to-date
2. Delete and remove the unused themes from your WordPress site
3. Download WordPress themes only from reliable sources
4. Get rid of the WordPress version number from the header.

Find more information on How to Detect Malware in WordPress Theme

Update WordPress plugins

WordPress users are spoiled for choice when installing a WordPress plugin. Choose all the slots, and you will have several choices of plugins for your niche, both free and premium.(See our list of best wordpress security plugins 2024)

One thing users should be careful about when selecting a plugin is the different pieces of unwanted code that are embedded in these plugins. To prevent from future threats, keep below-given tips in mind:

1. Keep all WordPress plugins up-to-date
2. Delete and remove unwanted or unused WordPress plugins
3. Get plugins only from reputable sources
4. Consider replacing old plugins with newer alternatives
5. Think twice before installing thousands of WordPress plugins

Regarding your plugins, we advocate following these recommendations:

Install only the plugins you need. No need to keep modules on your back office if you do not use them. We must therefore regularly sort and remove all those who are not active and whose you no longer need. This allows you to optimize the loading time of your pages and decreases the overall weight of your site.

Download and activate only plugins that are regularly updated. When downloading a module, you will be able to see the date of the last update. So be careful to always check the operational team behind the development of a plugin.

Ask about the quality of the plugins you download. Do not rush into downloading an extension. If you do not know it, take some time to learn about its quality. **Check customer reviews and download number**. You can find all this information on WordPress.org. You can also search on the internet the official site of the plugin as well as that of the creators to know more.

Secure your WordPress Database

SMEs are more concerned with cyberattacks than large companies because they are more vulnerable, especially e-businesses that hold sensitive data. A cyberattack can lead to cybercrime, whether at the IT (site blocking), financial, or reputation level (user data may be exposed). Cyber Attackers can perform this attack by accessing your database so take steps to reduce the attack surface or entry points for attackers:

Also Read – Repair WordPress Database & Fix Corrupted Tables

Change the prefix in the database

A very simple way to protect yourself is by using alternative prefixes for the names of the tables. If you install WordPress default, all tables in your database will take the prefix wp_: wp_posts, wp_postmeta, wp_users, wp_usermeta, wp_comments, etc.

A good security practice is to change this prefix wp_to a different prefix. For example, we could decide to choose the prefix 1a2b3c_as an alternative.

Also Read – How To Export WordPress Database Phpmyadmin

Schedule daily Backup of the WordPress database

You must always install and set up a WordPress database backup for your site. This allows you to safely restore your wordpress site from backup in case of

This allows you to safely restore your wordpress site from backup in case of problems.

Many users lose access to their WordPress dashboards due to hacking or plugin error. In these cases, most of our tutorials, recommend to always make a full WordPress database backup, which will save you a lot of inconvenience.

Plugins to backup your database table

UpdraftPlus WordPress Backup plugin provides service to recover and save your sites. If you manage multiple sites, then take a look at this plugin, which you can link to WordPress by activating UpdraftPlus WordPress Backup.

Thanks to it, you will be able to do all your updates at the same time (and in one click), clean spam, backup databases, do security checks etc. This service also has a schedule daily Backup function (free and premium).

You may also use:

WP Database Backup

WP-DBManager

Use Secure WordPress Hosting

In this step of our WordPress security guide cum checklist we talk about the importance of ensuring your web hosting plan is working to keep your website as secure as possible. Make sure to choose a reliable managed Wp hosting provider such as Host & Protect with a team of experts on site to handle your website's security measures.

Some of the features your managed WordPress hosting plan should offer are:

- Data center security measures
- Server-side security systems, such as firewalls and anti-malware software
- Free SSL certificate
- Automated or managed backups
- Managed updates

Features To look for in a Web Hosting Provider

- **You get what you pay for**: if your website is primarily a hobby, this should not matter. However, as an essential business tool, it is often a bad decision to bet on the cheapest (or free Hosting plan) proposal that is offered.
- **Beware of pricing tricks**, the vast majority of hosting services offer low at the start of their contract prices, but then raise prices once the introductory period has ended. That can be 24, 36 or even 60 months after registering.
- **How reliable is the provider**, almost anyone can claim to be a true web hosting provider and simply resell the products of another provider. So look how long they have been providing hosting services to the clients. Do they have a contact address, who is the owner, if you are making realistic promises on the website, etc.
- **Know your limits**: How comfortable are you with creating your own website? Do you need external help to build it?
- **Consider the Web Developers**, so you do not need to configure WordPress,

Joomla, etc. To be online instead of these the website developers offer an interesting alternative. However, keep in mind that you will not be able to migrate your content easily, thanks to their proprietary platforms.

WordPress hosting service plays the most important role to protect your website against hackers and malware. Just make sure to keep WordPress secure by following WordPress security tips:

1. Use SFTP or SSH to transfer files between local and remote servers
2. Assign Correct WordPress file permissions to 755 folders and 644 files in bulk (according to the Code Reference)
3. Protect the WordPress wp-config.php and make sure it is not accessible by others
4. Prevent access or disable via .htaccess files license.txt, wp-config-sample.php, and readme.html
5. Disable Editing in Dashboard via the wp-config.php with the code: define('DISALLOW_FILE_EDIT',true);
6. Deny access to all files and folders through .htaccess by adding the following code: Options All -Indexes

By now, you have read our WordPress security guide checklist 2024 given above. So **let's get started below**!!

TAGS:

how to secure wordpress / security checklist / wordpress best practices / wordpress installations / wordpress plugins / wordpress security guide / wordpress security risks

JANUARY 3, 2024

PREVIOUS

« Convert Plus WordPress Plugin Vulnerability Exploit [FIXED]

NEXT

Parse Error: Syntax Error Unexpected in WordPress [FIXED] »

RELATED POST

Latest WordPress Plugin and Theme Security Update 2024

WordPress Cookie Stealing: Risks, Identify, Prevention [GUIDE]

WordPress Supply Chain Attacks – Recovery & Prevention [2024]

RECENT POSTS

Cyber Security

Latest WordPress Plugin and Theme Security Update 2024

September 12, 2024

Wordpress Exploits

WordPress Cookie Stealing: Risks, Identify, Prevention [GUIDE]

August 13, 2024

Wordpress Security

WordPress Supply Chain Attacks – Recovery & Prevention [2024]

August 7, 2024

Uncategorized

Polish SMBs Bombarded With Phishing Campaign – BREAKING

July 31, 2024

News

4000+ WordPress Websites Compromised – Dual Threat Analysis

Cyber Security

How Do AI-Based Malware Removal Tools Help in Cybersecurity?

Analysis

July 31, 2024

Cybersecurity?

March 29, 2024