WORDPRESS & SECURITY

The connection that you need to understand

WordPromise

www.wordpromise.com

WordPromise

As hacks and security breaches become more of a concern for anyone running a WordPress website, it's important to know you can drastically improve your security by using a few…

WORDPRESS SECURITY BEST PRACTICES.

WordPromise

- Today WordPress is the most dominant **CMS** that powers more than **30% of the web** because of its ease of operation and limitless customization and flexibility. It is believed that there are nearly 2 billion websites online today and WordPress is responsible for nearly **70%** of the CMS market.

- On average, 30,000 new websites are hacked each day. **WordPress** sites are easy target for attacks because of **plugin vulnerabilities**, **weak passwords** and **outdated version** of the software.

- Most WordPress admins don’t even know they’re vulnerable, but with various security measures and tools, **WordPromise** can help you **fix** common holes, stop automated attacks and strengthen user credentials.

Understanding the Threat

WordPromise

Unfortunately, there are people & systems actively working to hack websites. There are many type of hacking from low to high end but they're unlikely to target your personal WordPress website. You may be tempted to personify attacks, but the reality is, a **"hacker"** is more like a mindless robot. By robots, we mean **"bots,"** or automated code that has a connection to the internet. Just like a robotic arm at a manufacturing plant is programmed to do specific tasks, these bots work every second of every day to perform their programmed tasks as often as they can, on as many sites as they can.

The goal of attacks is often to make the attacked site into yet another bot that can be given tasks. The tasks can range from attacking other sites to sending spam or phishing emails. In other words, these bots don't know what your site is about nor do they care. To the creator of the bot, each compromised site gives them access to more resources to create a revenue stream in one way or another.

Why Would Someone Want to Hack My Website?

WordPromise

There are currently tens of millions of websites on the web. **WordPress powers about 27% of them**. Unfortunately, the sheer number of WordPress sites makes it a target. Recently, **Sucuri** released a **Hacked WordPress Report**, with roughly 78% of the sites they worked last year were WordPress Sites and found that in most instances, compromises had little or nothing to do with WordPress core. Instead, WordPress compromises had to do with improper deployment, configuration and overall maintenance by the webmaster, host or the Website owners.

Even with these known WordPress security issues, WordPress is SECURE if you keep it up to date and some of the WordPress security best practices.

WordPromise

With so many threats to your website, it's important to make your WordPress site as secure as possible. Running a **WordPress security audit** of your website helps you prepare for and prevent successful attacks on your site.

You can't protect your site from every possible issue, but you can make sure you're prepared for the most common threats by running a WordPress security audit.

WordPromise

Website security is a complicated subject and you don’t want to go at it alone, especially if you’re not quite sure how everything works. **WordPromise** provides instant support so you know our team is ready to help you when you need it.

Call us at +91 9811401177 or email at info@wordpromise.com

For more info: https://www.wordpromise.com

WordPress websites are not set and go system. Once your site is launched, it requires ongoing maintenance and frequent updating. Much like the software on your computer, regular plugin, theme and software updates are released to fix security issues, make improvements, fix bugs, etc. but they're not as easy to adopt.

WordPromise

Without a qualified **WordPress expert team** or a developer, overseeing these updates, a website owner faces numerous issues from plugin incompatibility and theme breaks to **security risks.**

WordPromise

What is the RISK?

- Core Framework
- Plugin and Theme Incompatibility
- Security Vulnerabilities
- Server Level Safeguarding
- Login & Other Functional Checklist

WordPromise

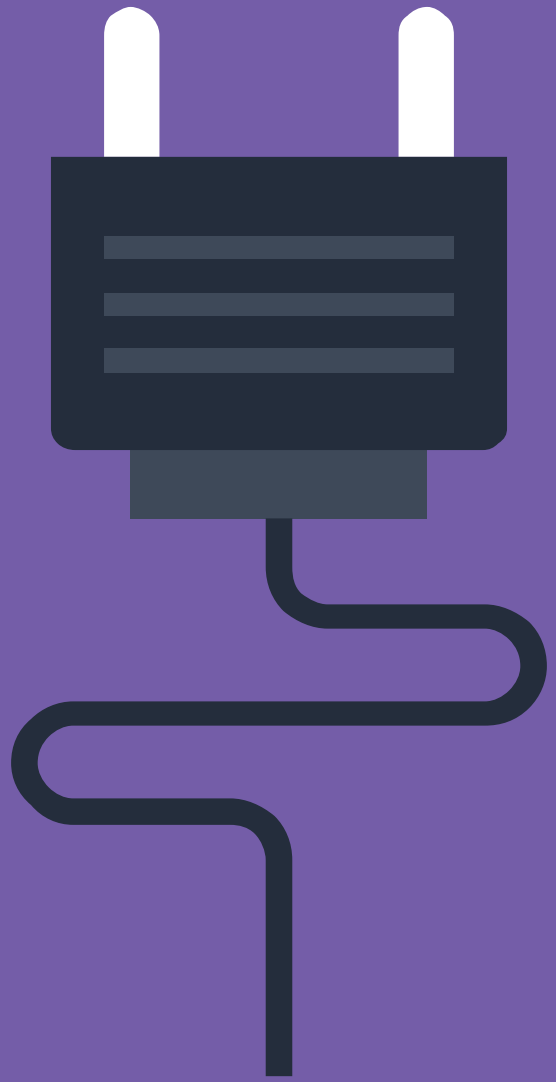
It is now more important than ever to keep your site up to date keeping in mind the number of threats WordPress has got as the most popular CMS application used among website industry.

Always backup database and your site before updating WordPress and don't neglect updates. The longer you wait to update to the **next version of WordPress**, the more you put your site at risk to be exploited by hackers or experience significant issues or bugs if your site is multiple versions behind the latest release.

WordPromise

One of the advantages of WordPress is that it's open source, so developers are contributing and creating new plugins and improvements all the time. The downside, however, is that a plugin created by one development team may not work well when paired with a plugin written by another developer.

This is called plugin incompatibility — updating one plugin may cause another to break or malfunction.



WordPromise

As for security, when a vulnerability is found in the version of a plugin or theme being used on your site, a developer can take quick action to limit any exposure.

With more than 49,000 WordPress plugins available in the official directory, vulnerabilities can go undetected and cause system compromises for years.

With a development team or developer handling the maintenance of your website, you can prevent malfunctioning systems and security issues, and ultimately avoid large development costs down the line.

Common Security Vulnerabilities

WordPromise

- Use a strong password with the help of a password manager.
- Two-Factor ALL THE THINGS.
- Have a reliable WordPress backup plan
- Use secure file permissions.
- Use sFTP whenever possible.
- Use SSL on all of your WordPress sites.
- Keep your WordPress site and everything on it up to date.
- Activate WordPress Brute Force Protection.
- Run scheduled malware scans.

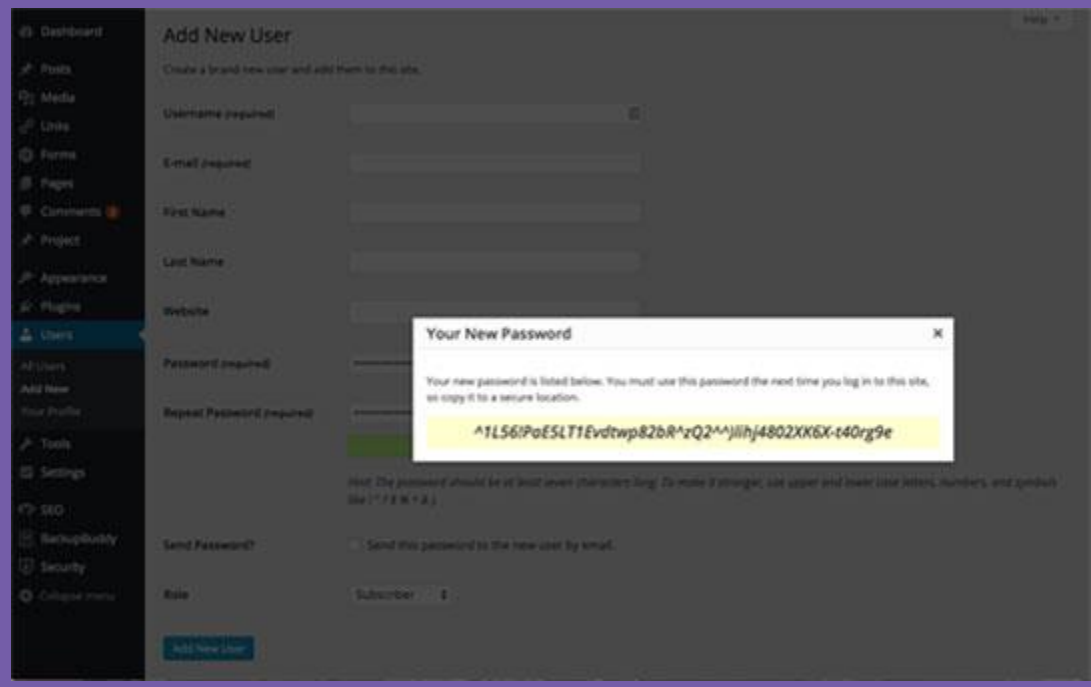
WordPress Password Security

WordPromise

ENFORCE STRONG PASSWORDS FOR ALL USERS

Passwords are a critical component of a solid WordPress security strategy. Our tools and configurations makes it easier for you to **enforce strong passwords**, so you can have greater WordPress password security.

Use strong password enforcement settings to add a strong password generator to user profiles, enable password expirations and control the minimum user role for strong password roles.



WordPress Two-Factor Authentication

WordPromise

EXTRA PROTECTION FOR WORDPRESS USER LOGINS

With WordPress **two-factor authentication**, users are required to enter both a password AND a secondary code sent to a mobile device such as a smartphone or tablet. Both the password and the code are required to successfully log in to a user account.

Two-factor authentication adds an **extra layer of WordPress security** to verify it's actually you logging in and not someone who gained access (or even guessed) your password.

WordPress Backup Solution

WordPromise

Hackers are constantly coming up with new ways to access your site. No matter how secure your site may be, it's still possible something can happen.

For this reason, when you are going through your **WordPress security audit**, it is very important that you have a **WordPress backup solution** as part of the security plan for your site. Using a WordPress backup plugin such as **BackupBuddy** is a good way to quickly get a solid WordPress backup solution up and running.

Use Secure File Permissions

WordPromise

How secure is your site if anyone can view or write to your server files? It's not. **Secure WordPress file permissions** are a must.

What you're actually able to set may vary from server to server, but you can usually adjust file and directory permission through your hosts control panel and FTP client. You should have your files somewhere between 400 and 444. And your directories somewhere between 700 and 744. Our audit tools includes a way to quickly check the status of your file permissions if you're not sure.

Use sFTP Whenever Possible

WordPromise

If you edit files on your website, it's a good idea to start using **sFTP** rather than **FTP**. If you don't directly edit the code, make sure your web developer is using the highest security protocols for accessing server files.

sFTP is a secure form of the FTP command. sFTP ensures that data is securely transferred privately with the use of the **SSH2 protocol**. When using sFTP instead of the FTP, the entire login session, including the transmission of passwords, is encrypted. So it's much more difficult for someone snooping around on the network to observe and collect passwords.

Use SSL on all of your WordPress sites

WordPromise

What is **SSL**? Why should you use it? We've all seen the green padlock in our browser next to the URL we are accessing, but why is it so important? SSL stands for **Secure Sockets Layer**, and creates an encrypted connection between your web server and your visitors' web browser. HTTPS stands for Hyper Text Protocol Secure. When using HTTPS if anyone is able to intercept it, they still won't be able to decipher it because it's encrypted.

SSL certificates range in price but are absolutely necessary to keep information on your website secure. There are also several places to buy SSL certificates, but the easiest route is to buy it from your host, and let them install it.

Keep Everything Up To Date

WordPromise

Keeping up with **WordPress maintenance** is the final part of having a solid WordPress security strategy. You have to do regular maintenance on your WordPress website, which means actively keeping up with updates to WordPress core, themes and plugins. Version updates often have important security patches and bug fixes, so it's important to always run the latest version of WordPress and any themes or plugins you're using.

- Keep WordPress core up to date.
- Keep plugins and themes up to date.
- Regularly update your passwords.
- Routinely audit your sites for plugins, themes and users that aren't being used, and remove them.

Preventing Brute Force Attacks

WordPromise

WordPress **brute force attacks** refer to the trial and error method of entering multiple username and password combinations over and over until a successful combination is discovered. The brute force attack method exploits the simplest way to get access to your website: your WordPress login screen. WordPress, by default, doesn't limit login attempts, so bots can attack your WordPress login page using the brute force method. Even if a brute force attack is unsuccessful, it can still wreak havoc on your server, as **login attempts** can overload your system. While you're under a brute force attack, some hosts may suspend your account, especially if you're on a shared hosting plan, due to system overloads.

Run scheduled malware scans

WordPromise

Keep tabs on potential **malware infections** with scheduled malware scans.

Malware scan offered in our audit services give you a report on your website's malware status along with several other blacklisting statuses.

Protect your site with an automated malware scans.

Other Common Security Checks

WordPromise

- Trusted Devices with Session Hijacking Protection
- WordPress User Security Check
- 404 Page Detection
- File Change Detection
- Lock Out Bad Users
- Away Mode
- Hide Login & Admin
- Database Backups
- Email Notifications

WordPromise

In addition to these best practices, there are many other things you can do to secure your WordPress website further.

Here are some quick recommendations…

- If possible, avoid cheap Poor-Quality or Shared Hosting. Use a reputable WordPress hosting provider.
- Don’t use Plugins and Themes from Untrustworthy Sources. Just because a plugin or theme is deactivated doesn’t mean it’s not a threat. You need to delete the plugin entirely.

WordPromise

Good WordPress Security is About Minimizing Risk

While these WordPress security tips can significantly decrease the chances of a successful attack, there is always that small chance you will fall victim to a cyber attack.

Good security is about minimizing risk. If anybody tries to sell you a 100% secure solution, they're scamming you.

Follow these WordPress security practices in order to minimize security risks.

Or hire an expert from **WordPromise** to take care of them.

In Conclusion...

WordPromise

While WordPress security issues do exist, most can be avoided with **WordPress security best practices** and an awareness of the potential security risks.

Armed with knowledge and strategies to protect your WordPress site, you can greatly minimize your vulnerability to hacks and keep your WordPress site safe and secure.

Contact **WordPromise** for consultation and get your WordPress Website Security Audit done today!

Call us at +91 9811401177 or email at info@wordpromise.com
For more info: https://www.wordpromise.com