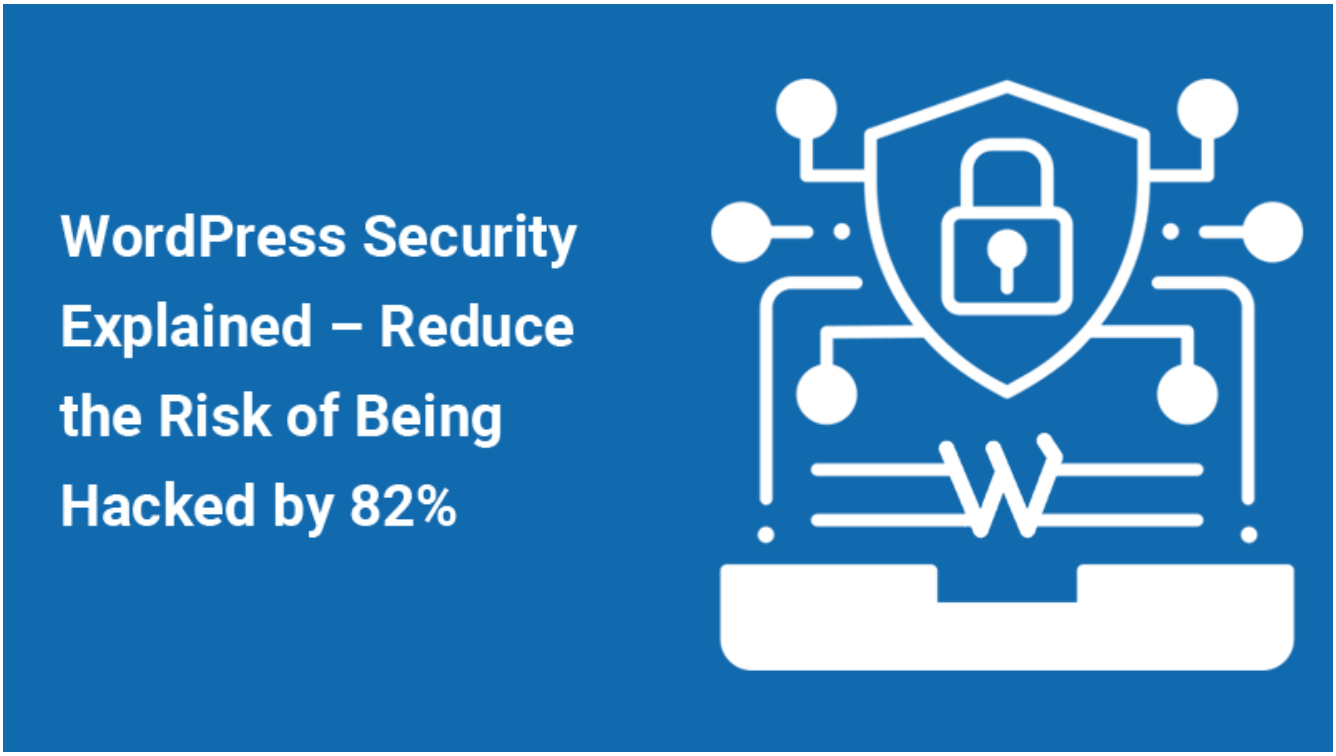
WordPress Security Explained – Reduce the Risk of Being Hacked by 82%



In 2023, the WordPress is still #1 fastest growing website platform and the best content management system currently available. Approximately 42% of all websites online are based on WordPress. Fortune 500 companies, online shops, banks and even governments are using WordPress, so no wonder that this platform is widely targeted by hackers, especially in the past few years.

Statistics and my experience are showing, that 90% of WordPress breaches are caused by "external" factors. WP themes, plugins and website hosting companies are the main source of security issues. WP core files are almost bulletproof and the development team behind WordPress is diligently working on further security improvements.

Need to mention that there's a big difference between attacks on a randomly picked sites and attacks where someone is specifically targeting some business. Random cyber attacks are happening on a daily basis and usually they are on a much smaller scale. On the other end, we have complex attacks where some company is being targeted by competitors for instance and very often the main goal is data theft. In some cases, complex attacks may be prevented only by a experienced WordPress developer or a cyber security professional.

Read the WordPress security guide below and reduce the risk of being hacked for more than 82%.

1. Basic rules on how to find a secure and reliable hosting for your WordPress website

The most common mistake you can make is to purchase one of those cheap hosting packages, $3-$10 dollars a month. **With cheap hosting providers, the disaster is guaranteed!** It's just a matter of time. As usual, "affordable" hosting servers are full of security loopholes and there's absolutely no point to even try to implement some protection on a website level.

No matter what you do, the website files or a database may still be vulnerable. So, the golden rule is stay away from cheap hosting plans. With a decent and properly managed hosting, there's a possibility that you will never end up hacked.

- Based on my experience the biggest names in the hosting market are actually not the best choice.
- The so called "Managed WordPress hosting" is nothing else than a marketing trick. Regular Linux/cPanel hosting is the best solution when it comes stability and management.
- Domain registrars that are providing hosting as a secondary/additional service will certainly not be able to meet the security requirements. Tested and proved over the years.
- The most reliable hosting companies do not have time to deal with anything else beside hosting.
- Hosting reviews are not credible source of information.
- Web developers and people from a marketing world have the real info. Read their forums and

find out what hosting companies they are using.

- Avoid shared hosting plans that are under $25/month .
- When it comes to dedicated servers, the average pricing for a good and quality server is over $200/month.

If you are still not sure how to find the best hosting for your website, contact me today. I can analyze your website/traffic, migrate the site and make it super secure.

2. Backups

No matter what goes wrong, backups are the best insurance. During the backup process, the server is saving a copy of your database and site files so that you can download everything to your PC or if needed restore the site within 10-20 minutes.

Even though, the hosting companies are doing backups on a daily basis, it's highly recommended that you have your own copies saved locally on multiple devices (PC, USB stick, online storage etc..). **Sometimes, days or weeks may pass until you notice that site is infected. That's why you should always keep the latest backup files for at least a month or two.**

You can manually backup your site by going to your hosting cPanel > Backup wizard. After the backup is generated, you can download the zipped file.

Beside backup methods mentioned above, I suggest to also use WordPress backup plugins, especially if

you don’t have time to do manual backups on a regular basis.

I recommend UpdraftPlus plugin and a BackupBuddy. Both plugins have option to save files directly to online cloud storage (Dropbox, Amazon, Google drive etc..).

3. WordPress Themes & Plugins

In order to change the look of your website, you have to download some WP theme online and install it. **By installing the theme or a plugin, you are actually adding third party code to your website.** In order to minimize security risks, use premium or free themes/plugins only from trusted sources.

A few years ago many popular themes and plugins were using an image resizing script called TimThumb until hackers figured out how to exploit it. Thousands and thousands of websites ended up infected with a same malware.

You can significantly improve your website security by using themes and plugins created by reputable companies or developers.

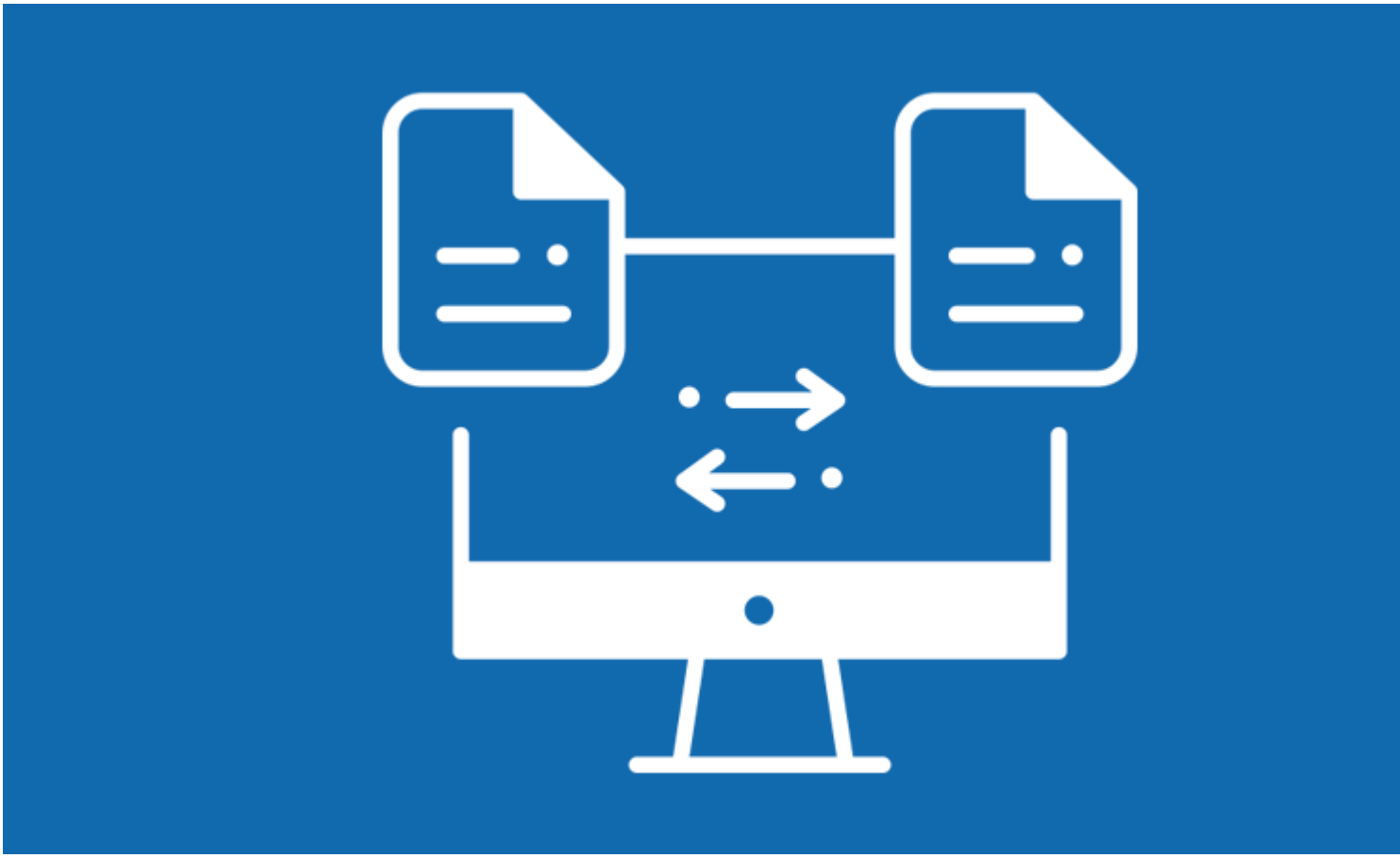
One of the places where you can find premium themes, plugins and other resources is Themeforest market. The good thing with this market is that every author is rated and you can quickly figure out is it safe or not to use products created by certain developer or a company.

Also, I suggest to check the comments related to some product before you make a purchase.

I will list only a few sources because I cannot guarantee anything before I see the code under the hood. Always check the rating and comments!

- Themeforest WP Themes
- Themeforest WP Plugins
- WordPress Theme Repository
- Plugins created by Automattic
- Woocomerce Themes and Extensions

If you are paranoid about security as I am, than the best approach would be to use a custom coded theme where every line of code is thoroughly tested. As a WordPress Expert, I can do all the work for you, develop an entire website, optimize it and make it bulletproof.

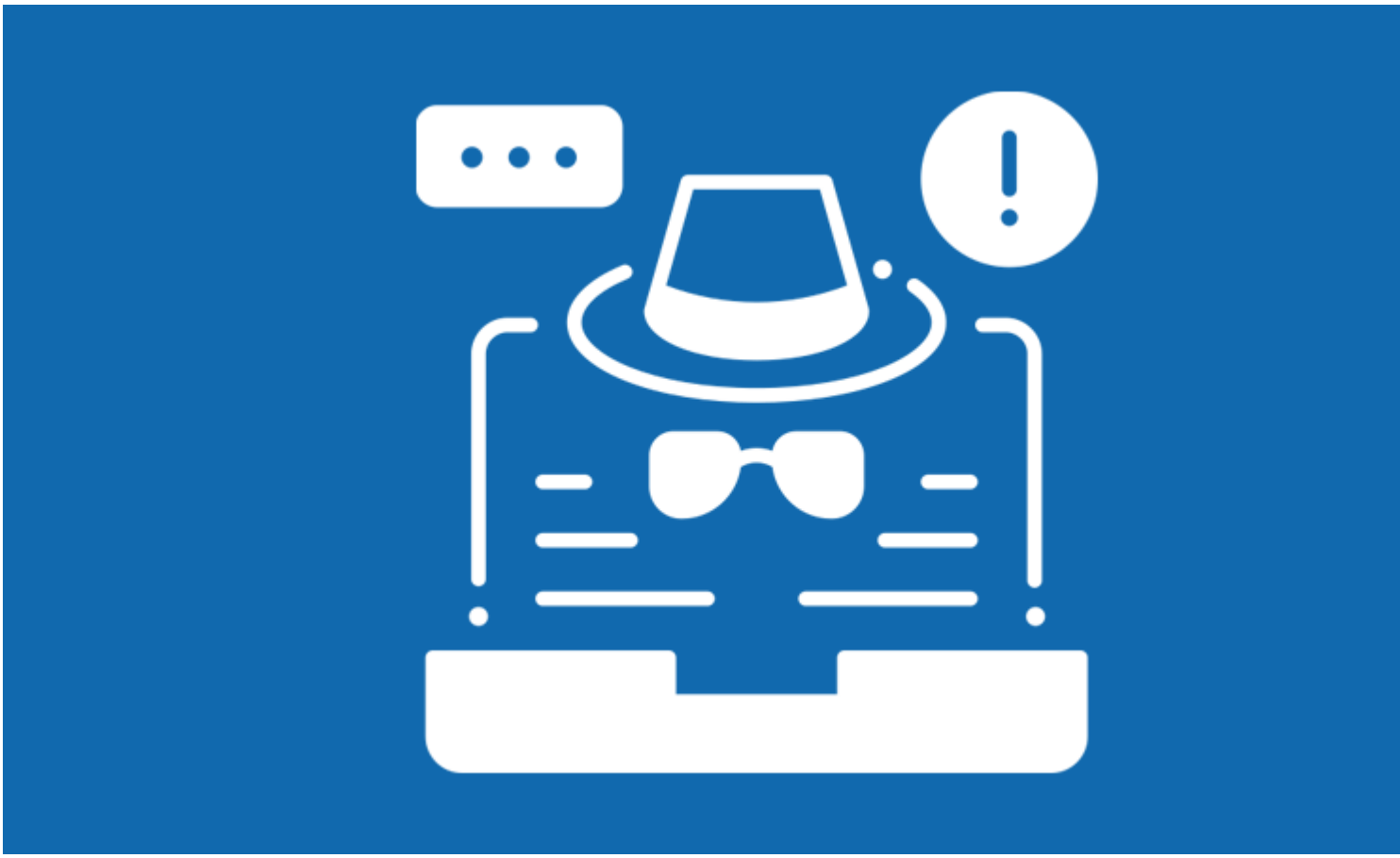


4. Updates

Updates for WP core files, themes or plugins usually contain code improvements, bug fixes or some additional features. Hackers are always busy trying to find a hole from where they can get in and take over the site. And as the time is passing by, there's a possibility that they will manage to exploit some piece of code written by inexperienced developer. It's crucial for security to always keep your website regularly updated.

You can update your WP core files and plugins in WP Admin dashboard > Updates. Some WP themes

can be easily updated with 2 clicks and if the theme is heavily customized, all the work should be done by a WordPress expert.



5. The Human Factor

People are the biggest security loophole. A few months ago I was hired by some big company to do content and layout changes. When I requested the WP admin log in credentials, their username was admin and the password was admin12345. I cannot believe how things like this are still happening in 2022. Strong password is the first layer of defense against unauthorized access.

If you are not sure how to create a strong password, use a password generator tool. This tool will mix letters with special characters, numbers and symbols so no one can easily guess the password or hack it with many different methods (bruteforce etc..).

The next important things you should consider are your PC, tablet, phone, all the devices that you're using to log in to your site. If your PC is infected, your passwords may be hijacked during the log in. Use a high quality antivirus with integrated firewall and regularly scan your PC. Also, I do not recommend to save your passwords in browser or to use any kind of password management tools.

Strong passwords are complex and long, so I suggest to save them to Excel or a text file that will be hidden somewhere on your PC. Remember the last 4,5 characters of your WP password and remove them from Excel file so that one can log in even if that file is compromised. Use the same trick for

your email and a hosting log in credentials.

WordPress comes with five default user account roles:

- Administrator
- Editor
- Contributor
- Author
- Subscriber

Administrator role has access to everything, all the settings, files etc… The next three roles from the list above can add or edit pages and do other content related changes. Subscribers do not have access to WP Admin dashboard.

Very often I am noticing on clients sites that all employees have an admin account. That's definitely not secure. Only the developers and the site owner should have an admin user role.

The developer you hire to do some work on your website will have access to everything, including sensitive data. Recently I received a phone call from an online shop that had problems with WooCommerce plugin. New orders were coming in on a daily basis, but the funds were not visible on their PayPal account. Two minutes later I realized that their ex-developer changed the payment gateway settings and redirected all the funds to his own account.

Remember, not all developers are honest. Before you hire someone to work on your website, jump on a phone call and talk. The right person for this job should be able to quickly within minutes process all the info and provide solutions and suggestions on how to fix or improve certain parts of your website. Experienced and trustworthy developers have big portfolio and big clients.

Don't forget to remove all user accounts associated with your ex-employees! (WP Admin > Users > hover over account that you would like to remove and click delete).

6. Content Delivery Networks

Content delivery networks can help you to reduce the bandwidth costs and improve the website loading time. Your website may be hosted somewhere in Texas, but if the CDN is enabled, all requests (site files and other data) will be served from a CDN server that is near your location.

Every CDN comes with firewall and other security features that can prevent certain types of cyber attacks (DDOS, XSS etc..). Basically, CDN is filtering all the data and traffic between your hosting server and a website.

By enabling CDN, you will have an another layer of security and make you site much safer.

I recommend StackPath and a Cloudflare CDN.

7. Additional Security Features

There are a few more security features that you should implement in order to strengthen the security of your website:

- Hide WP Admin Log in – The default WordPress admin URL is example.com/wp-admin. This URL should be renamed to something more random and unique. example.com/john3920 for instance. This new URL won't be visible anywhere and you will be the only person that will know how to log in.
- WordFence Security Plugin – This is the most popular security plugin on the market. It comes with endpoint firewall and a malware scanner.
- 2 Factor Authentication – When you try to log in, 2FA feature will send a temporary code to your email or phone and once you enter the code to the log in page, you'll able to access the website. I suggest to enable 2FA for both WordPress and your hosting account. This feature can be found in premium version of WordFence.

As mentioned in the beginning of this guide, the most important thing is to have a very secure and reliable host. The hosting server is basically the foundation of every website. If the server is not properly managed and maintained, the hackers will simply bypass all security measures and find a way to get in.

About the Author

Nick, the WordPress Expert. 15+ years of experience with web / WordPress development and security. Trusted by many successful companies and high traffic sites. Nick is a one-man army that prefer to work alone. As he explained to us, the key to his success lies in the fact that outsourcing was never an option.

Nick can be reached online at https://wp-expert.net/

This articles has been featured at: https://www.cyberdefensemagazine.com/wordpress-security-explained-reduce-the-risk-of-being-hacked-by-82/