12 Reasons Why WordPress Hacks Are Not a Big Deal

All vulnerabilities and potential hacks work to the hacker's advantage. They do not favor webmasters. It is harsh, but true. WordPress hacks are no exception.

There is a hacker attack somewhere in the world every 39 seconds. Worse is the majority are WordPress HacksMany wordpress websites are compromised everyday, and webmasters go in a deplorable condition. Hacked website makes an adult cry like a toddler.

Worst thing is most of the wordpress webmasters do not have any backup at all. This makes the situation uncontrollable. The damage is almost permanent if security professionals fail to recover the website.

Top 13 WordPress Mistakes

So that makes sense talking about why wordpress hacks are so common, and also why they are so successful. You must avoid the grim mistakes that make your wordpress website prone to attacks. If you have to keep your wordpress website safe from criminals you must avoid bad wordpress security practices or wordpress mistakes. Here are the 13 of them.

1. Little or zero maintenance of your wordpress website is one of the most common mistakes. One example is not updating the plugins or themes.
2. Not backing up the database and files.
3. Absence of malware checks, security scans, security plugins, and security monitoring.

4. Not being able to limit the login attempts.
5. Not using the sitewide secure socket layer (SSL).
6. Usage of weak passwords
7. One common mistake is to use the default user admin account instead of using a custom name.
8. Many of us add too many admins. We must use caution when giving the user privileges.
9. Many of us do not use two-factor authentication (2FA).
10. Do not use WordPress plugins that come from untrustworthy sources.
11. We sometimes use wordpress themes from unreliable sources.
12. Not using the latest PHP version is a fatal mistake. It makes your website utterly vulnerable.
13. Choice you make for hosting is paramount in Wordpress. Do not fall for the trap of cheap, low-quality and shared hosting.

However, the above list could be more comprehensive.

Yet it does provide the baseline. It provides the baseline to build upon the strong wordpress website with least or zero number of loopholes. Stay away from the worst wordpress security practices to upgrade the security posture of your wordpress website.

Automated Tools

Small businesses often have a limited budget and not good enough security knowledge, let alone the staff. That is why they tend to overlook website security. It is not even in their priority list.

If you have a small business or startup and have no idea about what powers your website, confirm it as soon as possible. You may ask your web designer.

One other option is to use some tool like Builtwith. Go to this website's homepage. You will see a search bar at the front. Just give your website URL there and press enter. The tool will tell you what system empowers your website.

Also, there is a browser extension called Whatruns. It serves the same purpose.

Here is what Scott Ikdea, a senior correspondent at CPO magazine, expresses his thoughts in the following words.

“The relative ease of attacking a smaller business has become such that it’s now perceived as being worth a hacker’s time and effort in more cases – particularly when smaller businesses don’t patch out known vulnerabilities that hackers can use automated tools to quickly scan for and exploit.”

The use of automated tools makes businesses easy targets for hackers.

WordPress is a hot Content Management System

WordPress 7.0 was born in May 2003. That came with no plugins, no widgets, and no spell check at all. An incredible evolution of this hot content management system has made it the love of writing for many old bloggers. This evolution over time has been nothing short of olympian.

It currently is one of the fastest growing content management systems. WordPress empowers almost 34% of all websites in the world. It has a content management system market share of almost 60%. BuiltWith enlists at least 24,808,989 live websites that use WordPress.

What is more surprising is the number of new websites built every day. The figure is larger than 800.

Similarly, wordpress developers throughout the world, build new wordpress plugins every day. Estimates have it that almost every day 55,000 new plugins enter the market.

Rules of Checks and Balances

The transition of worst security practices into best security practices is a weird switch. It is just like acknowledging the presence of a beast in your room since day one. You had been unaware of it and now it has materialized for you.

The plan to eliminate the creature from your room is a must-have. You must begin keeping tabs on all your digital assets. Your company website falls under the same category.

What we are trying to say is that the company must be involved in website security. It is more crucial than we think.

Let's say you have hired a consultant or outsourced website security to an outside agency. This is not all. You should also have an internal employee or staff that crews the ship. Here is what every web master must remember. The ability to act on knowledge is the real power. Checks and balances should always rule, no matter what. It is undeniable.

The WordPress Hacks

Hackers or crackers can attack and break into your website in numerous ways. WordPress, as we know, empowers more than 30% of the websites. Bad guys are trying to discover new WordPress vulnerabilities, all the time.

They embrace any opportunity that hinges on a set-up-and-forget mentality. Be it wordpress comments, old and insecure wordpress versions, weak passwords, themes, plugins, or contact forms. They do not miss any chance to ruin your life.

A Sucuri report reveals that WordPress suffered 90% of CMS cyber attacks in 2018. It was more than that 0f 2017, which was 83%. They also observed that the other key findings in CMS exploits are related to following things:

- Security configuration issues
- Improper deployment
- Lack of security knowledge
- Lack of security resources
- Overall website maintenance
- Broken authentication
- Broken session management

In short, the passive approach to website security makes you swim in dangerous waters. It leaves you unequipped and unsuspecting of any wordpress hacks that have already occured. Weeks turn into months, and months morph into years and the incident is not even discovered. Remember, what we said in the start. In the world of attackers, every vulnerability and potential exploit works to their advantage.

Security Mind Making is Critical

So are you thinking how to make that beast out of the room? Well, it is obvious that the beast would not be able to pass through the little door you have in the room.

You have to tear down the wall, lead the beast out and then build the wall again. You must approach the worst security practices of WordPress the same way.

So it is time to clean up the dung, if you have a wordpress website powered by a set-up-and-forget mentality.

Best WordPress Security Practices

1. Maintain WordPress Website.
2. Keep updating your themes, plugins, and also the WordPress version.
3. Do take the backups of databases and files, frequently.