



The complete guide to

WordPress Security

Web Security Best Practices
to Safeguard Your Site

May 2023

Introduction

Websites are vulnerable to cyber attacks, and WordPress is a popular target for hackers due to its widespread use. WordPress is the most popular CMS in the world because it is user-friendly, customizable, open-source, and SEO-friendly. It powers over 40% of all websites on the internet, its popularity making it a prime target for cybercriminals who seek to exploit vulnerabilities to gain access to sensitive information, steal data, or take control of the website for malicious purposes. In fact, Google blacklists around 10,000+ websites every day for malware and around 50,000 for phishing every week.

Website security is especially vital for the healthcare and biopharma industry to protect sensitive patient data, maintain trust, comply with data privacy regulations, and safeguard valuable intellectual property. A security breach could result in legal liabilities, reputational damage, and financial losses, making robust website security a critical requirement that cannot be overlooked.

Table of Contents

04	Getting Started with WordPress Security
05	Account Login Security
09	Security Monitoring
12	Managing Plugins & Themes
161	WordPress Security Myths
18	Signs of a Website Breach
23	Website Recovery



Getting Started with WordPress Security

It's essential to implement proper security measures to ensure the success of your website. In reality, most hacks can be avoided by implementing a few basic security measures. Let's explore some steps that can be taken to secure your site.

4 Steps To An Effective WordPress Security Strategy

- 01 **Account Login Security**
- 02 **Security Monitoring**
- 03 **Managing Plugins & Themes**
- 04 **Website Backup Plan**

Account Login Security

One of the most significant advantages of using WordPress is its user-friendly interface, which allows virtually anyone to create a website. However, this ease of use comes with a downside: predictability. Experienced WordPress users know that any modifications to the website can be made through the wp-admin area, and they can easily access it by navigating to the wp-login.php page.

By default, every WordPress site has the same login URL, which does not require any special permissions to access. Consequently, the WordPress login page becomes the most targeted and potentially vulnerable component of a WordPress site.

How To Secure Your WordPress Login Account

1. Use Strong Passwords

The internet is flooded with conflicting advice on password security best practices. To dispel this confusion, let's examine the fundamentals of how using a robust password can enhance your WordPress security.

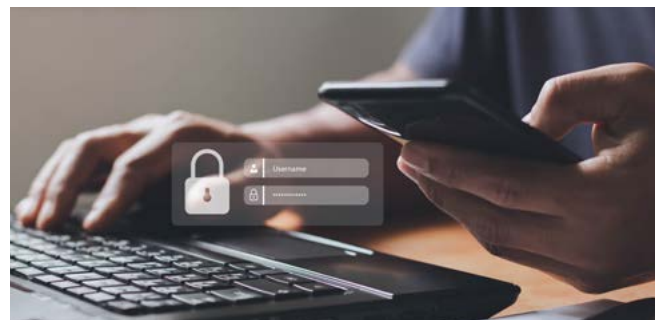
When crafting a password, the first aspect to contemplate is its length. By adding even one character to your password, you can drastically enhance the security of your login. A password that comprises a minimum of 12 random characters from a vast pool of options can significantly impede any attempts to crack it.

Regrettably, some cybercriminals are utilizing more powerful GPUs and CPUs to minimize the time required to break passwords. Therefore, to fortify your logins, it's crucial to consider your password entropy. The greater the password entropy, the more challenging it becomes for attackers to crack your password.

2. Refuse Compromised Passwords

Attackers frequently exploit compromised passwords to launch hacking attempts as it is quicker and simpler than using brute force techniques to try every possible password combination. If your password has been compromised and you reuse it on multiple websites, attackers could gain access to your account in just a few attempts.

A data breach generally involves a list of usernames, passwords, and other personal information that was exposed when a website was compromised.



3. Use A Different Password For Every Account

To enhance online security, it is advisable to create distinct passwords for each of your accounts and website logins. It cannot be overstated: using a different password for every site is crucial. When multiple users reuse passwords, the strength of your WordPress login security decreases.

It's essential to prioritize strong password requirements to enhance the WordPress login security of your website. Keep in mind that the security of your site is only as robust as its weakest link, hence the need for proactive measures.

Utilizing a password manager can assist you in tracking your logins and unique passwords. This tool eliminates the need to remember your passwords, enabling you to keep your online accounts secure.

4. Limit Failed Login Attempts

WordPress does not have any built-in feature to restrict the number of failed login attempts. This implies that an attacker can keep attempting an infinite number of usernames and passwords until they succeed. Without a limit on the number of failed login attempts, your site's security is at risk.

5. Limit Outside Authentication Attempts

There are alternative methods of accessing WordPress aside from using a login form. By utilizing XML-RPC, an attacker can execute numerous username and password attempts within a single HTTP request.

Attackers can utilize the brute force amplification technique to make thousands of username and password attempts via XML-RPC within a few HTTP requests. With the ability to use database dumps as a starting point and conduct a significant number of guesses per request, it underscores the importance of prioritizing WordPress login security.

It is crucial to note that the WordPress Rest API introduces new methods of authenticating a WordPress user when devising a security plan for your WordPress login.

Cookie authentication is a means of authentication that automatically stores a cookie when you log in to WordPress, enabling plugins and themes to execute a function on your behalf. By applying the protections you have implemented to wp-login.php, you can ensure that cookie authentication receives the same benefits.

6. Use Two-Factor Authentication

To access your WordPress account, two-factor authentication necessitates an additional code in addition to your username and password. There are various techniques for implementing two-factor authentication, but not all are created equal. It is recommended to refrain from using text as a method for two-factor authentication.

The National Institute of Standards and Technology no longer recommends the usage of SMS for transmitting and receiving authentication codes. Therefore, it is imperative to consider alternative methods of two-factor authentication to ensure robust WordPress login security.

It is important to be aware that certain websites necessitate the use of an email address as a username. In the event of an attacker hacking one of these websites, their next step would be to attempt to access email accounts using the stolen email addresses and passwords.

If any of your users or clients use the same password for all of their online accounts, they will be at risk of having their email account and two-factor email codes compromised if an attacker hacks one of the websites that require an email address as a username.



7. Passwordless Logins

Passwordless login is both secure and straightforward, making it more likely for individuals to secure their accounts. This login method enhances the security of your accounts and is more user-friendly than traditional credentials.

Without realizing it, you may already be using a type of passwordless login. For instance, if you are using Face ID or a thumbprint to unlock your phone, you are already using a passwordless login method. It is essential to note that a passwordless login does not necessarily mean that a password is not assigned to the user. For example, your phone still requires you to set a password or PIN, but it's not necessary to enter it every time you unlock your phone.

Purging Old Users

The importance of purging old users from your website cannot be overstated when it comes to maintaining robust website security. User accounts that are no longer needed or actively used can pose potential security risks, as they may be vulnerable to unauthorized access or account hijacking. These dormant accounts can be targeted by malicious actors who may exploit weak passwords, unpatched

vulnerabilities, or forgotten user credentials to gain unauthorized access to your website's backend, compromising sensitive data or even taking control of your website.

Regularly purging old users is a critical security measure to minimize the attack surface of your website. By removing outdated or unused user accounts, you reduce the potential points of entry for cybercriminals and limit the number of accounts that need to be monitored and secured. This also helps ensure that only authorized personnel have access to your website's backend, reducing the risk of insider threats or unauthorized access by former employees or contractors.

In addition to mitigating security risks, purging old users also helps maintain the integrity and accuracy of your user database. Keeping your user list up-to-date and only retaining active users improves user management, simplifies user permissions and access control, and enhances overall website performance. It is important to establish regular user account reviews and purge processes to ensure that your website remains secure, efficient, and protected against potential security breaches.



Security Monitoring

Is your website being closely monitored for suspicious activity that could potentially harm your online presence? This is a crucial matter to consider as daily events on your website could be indicative of malicious intent. In the following section, we will discuss the topic of security monitoring for your website.

WordPress Security Logs

Detailed data and insights about the activity on your WordPress website can be obtained from the security logs, which could help identify and prevent any malicious behavior on the site if you know what to look for. By including WordPress security logs in your overall security strategy, you can enjoy several benefits. In the event of a security breach, having access to accurate and comprehensive information from the security logs could greatly aid in quickly investigating and recovering from the attack.

WordPress security logging can assist in enhancing your security monitoring strategy in several ways, such as:

- 01. **Identify and put a stop to any malicious behavior on the website**
- 02. **Detect suspicious activity that can serve as a warning sign of a breach**
- 03. **Evaluate the extent of harm caused by the breach**
- 04. **Assist in the restoration of a hacked site**

1. **Brute Force Attacks**

The method of using trial and error to uncover usernames and passwords in order to gain unauthorized access to a website is known as a brute force attack. WordPress does not automatically track user login activity, leaving the website vulnerable to such attacks. Therefore, it is the responsibility of the website owner to ensure login security is monitored and protected.

Fortunately, brute force attacks are not particularly complex and can be identified through the website's logs. This requires recording login attempts including the username, IP address, and success status. Consistent failed login attempts by a single username or IP could be a sign of a brute force attack on the website.

2. **File Changes**

Despite implementing WordPress security best practices, there is still a possibility of your website being compromised, which means it has been subject to unauthorized and malicious changes. Therefore, it is crucial to regularly track file changes on the site and document them in the WordPress security logs.

Such entries would include new files added, files removed, and any modifications made to existing files. Once changes are recorded, it is essential to schedule regular audits.

While it is normal to notice new file change activity in your logs for various legitimate reasons, any unexpected changes should be carefully examined to ensure that they are not malicious. For instance, if you observe changes made to a plugin at the same time and date when you updated it, there would be no need for further investigation.

3. **Malware Scans**

It is important to not only perform regular malware scans, but also to keep a record of the scan results in your WordPress security logs. Although some security logs may only document instances where malware was detected, this is insufficient. Rapid detection of any site breaches is critical to minimize potential damage.

While it is satisfying to observe evidence of proactive security measures, recording malware scans serves a more practical purpose. Neglecting to document your scans may result in an inability to identify scan failures.

Failure to document unsuccessful scans may lead you to believe that your website is undergoing daily malware checks, when in fact the scan is not successfully completing.

4. **User Activity**

Maintaining a log of user activity in your WordPress security logs can prove to be crucial in the aftermath of a successful attack.

1. **Logins & Logouts**

One of the initial forms of user activity to keep track of is the login and logout times, as well as the location from which users access your website. By monitoring these details, you can identify compromised user accounts. For instance, if a user logs in from an unfamiliar location or at an unusual time, it may be worth investigating their account first.

2. **New Users**

Another user activity that should be documented is the creation of new user accounts. Hackers often create new admin accounts to conceal their actions, making it challenging to detect malicious activity on those accounts. While it may be simple to recognize unusual activity on your own account, identifying such activity on other user accounts can be considerably more complicated.

3. **Add / Remove Plugins**

It must be verified whether the new user has made any modifications to the site's plugins. It is crucial to keep a record of all plugin additions and deletions. If your website is compromised, the attacker can effortlessly add their own custom plugin to insert malicious code into the site. Even if they do not have server access, they can use a plugin to insert redirects on your site to be used in their spamvertising campaign. After their harmful code executes, they can delete the plugin to cover up any traces of their wrongdoing. Fortunately, with WordPress security logs, you will not miss any of this activity, as it will be thoroughly documented.

4. **Add / Edit Pages**

Next, it should be checked whether the new user has created any new pages or made modifications to existing pages or posts on the website. It is important to investigate whether the user has inserted any links that direct your website's traffic to other sites. This examination can also uncover any unsavory pages that have been added to the site, allowing you to take them down.



Managing Plugins & Themes

Maintaining the proper management of plugins and themes is crucial to ensuring the health of your website. In the following section, we will explore what this entails.

1. Update Everything

If your WordPress website is using outdated versions of WordPress, plugins, or themes, it is at risk of having known exploits present. Updates do not only include new features or bug fixes, but also provide security patches for known vulnerabilities. Although it is the easiest WordPress security issue to avoid, most successful hacks exploit vulnerabilities found in outdated software.

2. Automatically Patch Known Vulnerabilities

When your website is running software with known vulnerabilities, it provides hackers with the information they need to take control of your site. It can be difficult to keep track of every disclosed WordPress vulnerability and match that list to the versions of plugins and themes installed on your site.

3. Remove Unused Plugin & Themes

It's important to consider the PHP code on your WordPress site when evaluating potential security vulnerabilities. Hackers often exploit PHP code to gain access to sites, so it's crucial to reduce this risk by minimizing opportunities for exploitation. To do this, you can uninstall and completely remove any unnecessary plugins and themes from your WordPress site. This will limit the number of access points and executable code on your site, reducing the likelihood of a successful hack.

Furthermore, steer clear of using WordPress plugins that have been neglected by their developers. It's crucial to keep an eye on plugins that haven't received any updates for over six months, as they may have been abandoned. However, it's important to note that the lack of recent updates doesn't automatically mean that the plugin has been abandoned; it could simply imply that it is feature-complete and will only receive updates to ensure compatibility with the latest WordPress and PHP versions.

4. Only Install Software From Trusted Sources

To keep your WordPress site secure, it's important to only install themes and plugins from trustworthy sources. Trusted sources include WordPress.org, reputable commercial repositories, and directly from reputable developers.

Avoid using "nulled" versions of commercial plugins, as they may contain harmful code that could compromise your site's security. Even if you've taken measures to secure your site, installing malicious software can undermine your efforts.

If you come across a plugin or theme that isn't available on the developer's website, be sure to do your research before downloading it. Reach out to the developers to verify that the website offering their product at a discounted price is legitimate.



WordPress Security Myths

There is a lot of security advice available online from people who genuinely want to help. However, not all of it is accurate and some of the advice is based on WordPress security myths that do not provide any additional security to your WordPress website. In some cases, following such advice may increase the likelihood of encountering issues and conflicts.

1. You Should Hide Your /wpadmin or /wp-login URL (Also Known As “Hide Backend”)

The concept of hiding the wp-admin is based on the assumption that hackers cannot target what they cannot locate. However, if you change your login URL from the default WordPress /wp-admin/ URL, does that make you invulnerable to brute force attacks?

In reality, most plugins that offer Hide Backend features rely on security through obscurity, which is not a foolproof security approach. Although concealing your wp-admin URL may help reduce some login-related attacks, it is not a comprehensive solution.

2. You Should Hide Your Theme Name and WordPress Version Number

You may have heard that hiding your theme name and WordPress version can help to prevent attackers from breaking into your site. The idea behind this is that if attackers have this information, they will be able to find vulnerabilities and exploit them.

However, the truth is that there aren't actual people searching for specific theme and WordPress version combinations to attack. Instead, automated bots search for known vulnerabilities in website code, so hiding this information won't provide any real protection.

3. You Need to Rename Your wp-content Directory

The wp-content directory is a crucial directory in WordPress, housing important data such as plugins,

themes, and media files. Given the sensitivity of the data contained in this directory, website owners may feel inclined to rename it in an attempt to add an extra layer of security to their site.

However, changing the name of the wp-content directory is a myth and will not provide any additional security to your website. In fact, it can cause conflicts and issues, and the new directory name can still be easily found using browser developer tools.

4. WordPress is an Insecure Platform

The misconception that WordPress is inherently insecure is the most damaging security myth surrounding the platform. In reality, WordPress is the most widely used content management system in the world and has earned its popularity by taking security seriously.

Rather than a flaw in WordPress itself, the primary security vulnerability lies with its users. Many WordPress hacks can be prevented with minimal effort from site owners.

It's important to note that the most common cause of successful WordPress hacks is outdated software. To avoid this, it is crucial to keep everything up to date. WordPress offers automatic updates as an option, but some site owners fail to update their sites regularly, leaving them vulnerable to attack. When a hacker exploits a security hole, it is not due to a flaw in WordPress, but rather a flaw on the part of the user.



Signs of Website Breach

If you find yourself wondering whether your WordPress site has been hacked, it's important to seek quick answers. We will outline seven indicators of a potential infection and provide guidance on what needs to be done if it's discovered that your site has been compromised.

Detecting signs of a website breach early allows for prompt action to clean up your site and minimize the damage caused by the hack. Keep in mind that the signs of a website compromise may vary depending on the attacker's motive.

Below are seven different symptoms to be vigilant about when monitoring the security of your site.

1. You Should Hide Your /wpadmin or /wp-login URL (Also Known As "Hide Backend")

It may seem obvious, but changes to your homepage can be a clear sign of a hacked website. However, how often do you actually conduct a thorough check of your homepage? Many people often go directly to their login URL instead of their home URL. Once logged in, they update their site or edit a post, and then leave without looking at the website's home page.

It's important to note that some hackers' primary goal is to troll a website or gain notoriety. As a result, they may only make changes to your homepage, such as displaying something they find funny or leaving a "hacked by" calling card.

Therefore, regularly checking your homepage for any unauthorized changes can help you detect potential hacks early on.

2. Your Website Performance Drops

If your website feels sluggish, it could be a sign of a potential infection. Slowdowns may occur due to brute force attacks or when a malicious script is utilizing your server resources for cryptocurrency mining. Additionally, a DDoS (denial of service) attack can cause your website to slow down or crash, as it involves multiple IPs simultaneously sending requests to your site.

To determine if your site is running slowly due to a potential hack, you can check your server access logs for an unexpected surge in requests. Utilizing a web application firewall, such as the one offered by Sucuri, can also help protect your website against DDoS attacks.

3. **Your Website Contains Malicious or Spam Ads**

If visitors to your website encounter popups that redirect them to a suspicious website, it's likely that your site has been compromised by a hacker. The objective of this type of attack is to divert traffic from your site to the attacker's site, where they may engage in click fraud for Pay-Per-Click advertising.

What makes this type of hack particularly frustrating is that the popups may not be visible to you as the website owner. Hackers can design the popups to be hidden from logged-in users, reducing

the likelihood of website owners noticing them. Even when you log out of your site, the popups may not be displayed.

Furthermore, if you use an ad blocker extension in your browser, your ability to view the popups may also be limited. It's crucial to be vigilant and regularly check your website for any signs of unauthorized popups to promptly address any potential security breaches.

4. **Website Traffic Decreases**

If you log into your Google Analytics account and observe a significant decrease in website traffic,

it could be an indication of a potential hack on your WordPress site. A sudden drop in site traffic warrants further investigation, as it may be due to a malicious script on your site redirecting visitors away from your site, or Google may have already blacklisted your website as a malicious site.

The initial step is to examine your website's outbound traffic. To monitor this, your site can be configured in Google Analytics to track the traffic that leaves your site. One convenient method to monitor outbound traffic on your WordPress site is by utilizing a WordPress Google Analytics plugin. A

reliable Google Analytics plugin for WordPress will enable the ability to easily track specific activity with just a click of a button.

5. **Unexpected File Changes**

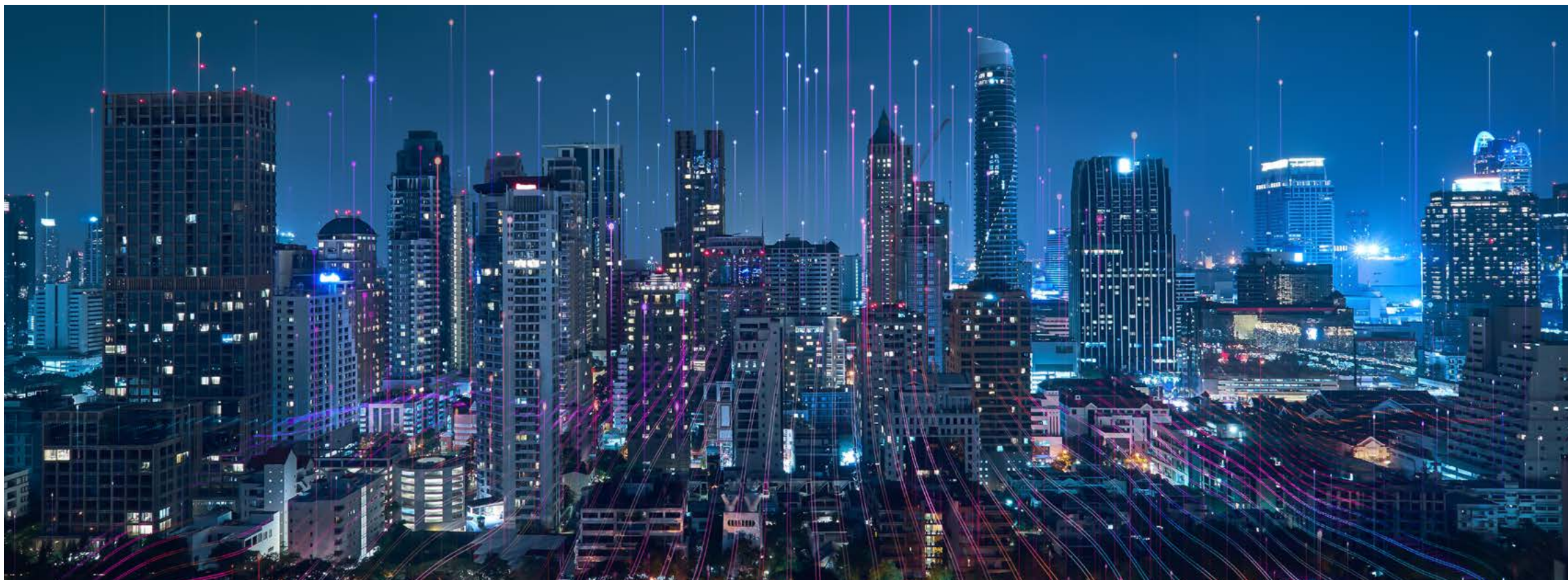
If you notice modifications, additions, or removals of files on your website, it could be an indication that your site has been compromised. Therefore, it is crucial to have a notification system in place that can alert you of any changes to your website files. You can investigate unexpected file changes by comparing the altered file with a recent backup version to identify any potential security breaches.

6. **Unexpected New Admins**

If you notice unexpected registrations of new admin users on your website, it could be an indication that your WordPress site has been hacked. Attackers can exploit a compromised user account to create a new admin user with malicious intent. With the newfound admin privileges, the hacker can potentially cause significant damage to your website.

7. **Removed Admin Users**

If you find yourself unable to log into your WordPress site, even after attempting a password reset, it could be a strong indication of a potential infection or compromise.



Website Recovery

If you're unable to access your website due to a complete loss or being hacked, it's important to have a backup strategy in place for a quick recovery. Restoring from a backup is often the easiest and fastest way to regain control of your website. Here are ten steps to creating a backup strategy and ensuring peace of mind.

1. Select a Backup Method

Look for a dedicated backup solution such as BackupBuddy.

2. Determine What to Include in Your Backups

Make sure your backups include plugins, themes, media, uploads, and your database.

3. Set Your Backup Frequency

Consider how often your website changes and choose a backup frequency accordingly. If you make daily changes, daily backups may be necessary.

4. Schedule and Automate Your Backups

Choose a convenient time for your backups and use a backup plugin to automate the process.

5. Choose an Offsite Storage Location

Store your backups in a separate location from your website's server for added security.

6. Scan Your Backups

It's crucial to scan your backups for any potential

infections, as a compromised backup won't be effective in cleaning your site.

7. Audit Backup Schedules

Regularly review and verify the functionality of your backup automations to ensure they are working as intended.

8. Know How to Restore

Familiarize yourself with the process of restoring your website from a backup, so you are prepared to do so when needed.

9. Understand Your Environment's Limitations

If your website is hosted on a poor hosting environment, make sure your backup strategy is tailored accordingly to ensure its effectiveness.

10. Be Ready to Migrate

In case of issues with your hosting provider, knowing how to migrate your site to a different host will give you the flexibility to move when faced with problems.

Conclusion: Simplifying the Complexities of WordPress Security

Ensuring the security of your WordPress website is a complex task that requires a deep understanding of web security principles, constant monitoring, and timely updates. The ever-evolving landscape of cybersecurity threats makes it challenging for individual website owners to keep up with the latest security measures and best practices.

Therefore, it is prudent to trust a web security partner to handle the job for you. A professional web security partner will have the necessary expertise, experience, and resources to implement robust security measures, conduct regular audits, and proactively mitigate potential security risks. They can provide 24/7 monitoring, timely software updates, and comprehensive security protocols to protect your website from the latest threats, leaving you free to focus on your core business activities without worrying about security vulnerabilities.

Investing in a web security partner not only helps safeguard your website against potential attacks but also provides peace of mind knowing that your website is in the hands of professionals who are well-versed in web security best practices. The complexity and constantly changing nature of website security make it essential to trust a reliable and knowledgeable partner to safeguard your website and protect your valuable digital assets for the long term.



The complete guide to

WordPress Security

Annalyse Madsen

Account Manager

amadsen@emagine.com

(508) 802-5550

emagine.com



Web Security Best Practices
to Safeguard Your Site

May 2023