11 Most Common WordPress Mistakes

And how to fix them

WP SUPERSTARS
WORDPRESS. SIMPLIFIED.

Introduction

We all make mistakes from time to time but when it comes to WordPress, there are some mistakes that can have devastating consequences.

But, the unfortunate truth is that these mistakes can be so easy to make, especially if you're just getting started.

Learning from your mistakes is important but if you can avoid some of these mistakes, you'll save yourself a lot of time and money in the long run.

In this guide you will learn exactly which mistakes to avoid and you will also learn exactly how to fix them, without any fuss or crazy learning curve.

We'll cover key mistakes around topics such as security, usability, SEO, technical setups and more but you won't get an overwhelming amount of information – just the key mistakes and how to avoid them.

You'll get simple solutions to big mistakes – sound good?

Let's dive straight in because your time is precious.

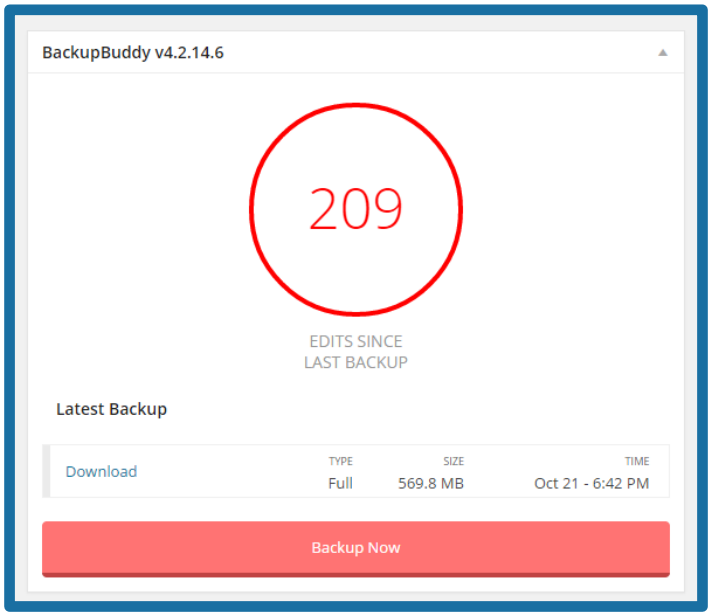
#1. You haven’t backed up your website

When was the last time you backed up your website?

Your web host may do regular backups for you, but not all web hosts do and there have been occasions where web hosts have dropped the ball. This has resulted in entire websites to be lost without any acceptance of responsibility.

You need to take control of backups yourself and ensure that they are done on a regular basis – full backups too, not just database backups.

There are various plugins available, both free and premium which you can use to easily backup your website. You can find a more detailed list in this post.



We have used a lot of different backup solutions over the years, including BackupBuddy which is a popular premium plugin. We currently use VaultPress which is an online tool that costs $5/month for basic backups.

A great free alternative is UpdraftPlus which comes highly recommended.

#2. Using a web host that buckles under pressure

Sounds easy doesn't it?

Pick a web host, install WordPress and everything will be fine. But the truth is that you have to carefully consider which web host you choose.

The $3/month price tag of some budget hosts sounds all well and good but the truth is that most of these web hosts buckle under pressure.

As soon as your website starts to receive simultaneous visitors, load times instantly skyrocket and that's a huge problem.

Why?

Just a 1 second delay in load times could potentially lower your conversion rates by 7% - that's a huge number for such a small amount of time. So this just highlights the ever increasing importance of investing a bit more money to get a better web host.

In order to deliver the best experience possible, it's worth using a CDN with your web host to further improve load times.

CDN stands for "Content Delivery Network". It's just a group of servers located at key locations around the world so it can deliver content to visitors from the closest location.

At WP Superstars, we host our website with Traffic Planet Hosting – they have great support, technical knowledge of WordPress (most hosts don't) and load times are seriously fast.

We also use MaxCDN to further speed up the site.

#3. Not using a caching plugin

WordPress is dynamic and database-driven: Every time a user visits your website, PHP code requests info from a database and uses it to build an HTML page.

“Caching” means storing those HTML pages to reduce database requests. Pages are only rebuilt as needed when something changes, giving your site a speed boost.

Some web hosts have their own caching functionality, but if yours doesn’t, you’ll need to get a plugin installed to take care of this.

There are a number of plugins you can use for this and they’re all free.

There are two we like in particular:

- W3 Total Cache – You’ll see a noticeable difference just by activating this plugin, although to get the most out of it you need to tweak the advanced settings which you should only do if you are comfortable.

- WP Supercache – Requires some initial setup work but the plugin is very straight forward and offers you a list of recommended settings.

#4. Uploading huge images when you don’t need to

Uploading images with huge file sizes can seriously slow down your websites page load times.

You need to optimize every image for the web before you upload it to WordPress. Most images can be compressed without causing a noticeable drop in quality.

We generally aim for each images file size to be below 100KB.

There are plenty of tools that can help you with this, like Photoshop for example but there are other tools you can use depending on the image file type such as:

- TinyPNG – PNG images
- JPEGmini – JPEG images

If you've already got a lot of large images in WordPress – don't worry, you don't have to optimize them one-by-one, there are plugins like WP Smush.it which will allow you to optimize them automatically.

For more information on optimizing images for WordPress, this post is a good starting point.

#5. You're not managing broken links and 404 errors

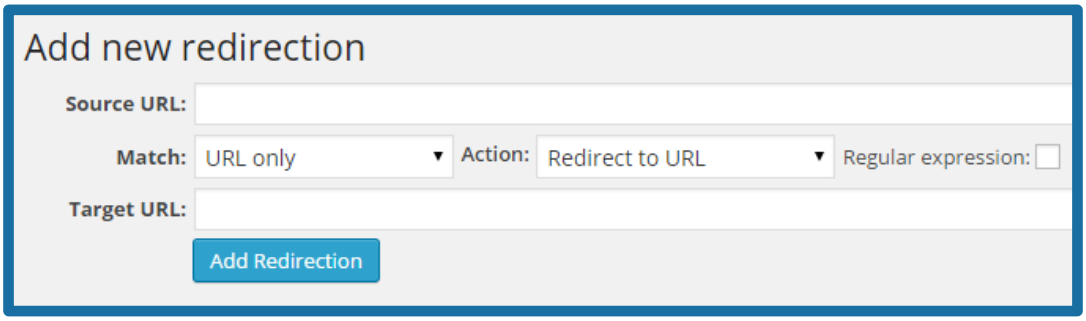
Whenever a URL changes you need to redirect the old URL to the new URL.

If you don't, users will be greeted by a 404 error and search engines will struggle to crawl your website.

This is a huge issue in terms of both usability and SEO.

There are a number of ways you can add redirects in WordPress but the easiest way is to use a free plugin called Redirection.

Just by activating the plugin, it will automatically add redirects whenever you edit the permalink for a post/page but you can also add redirects manually.

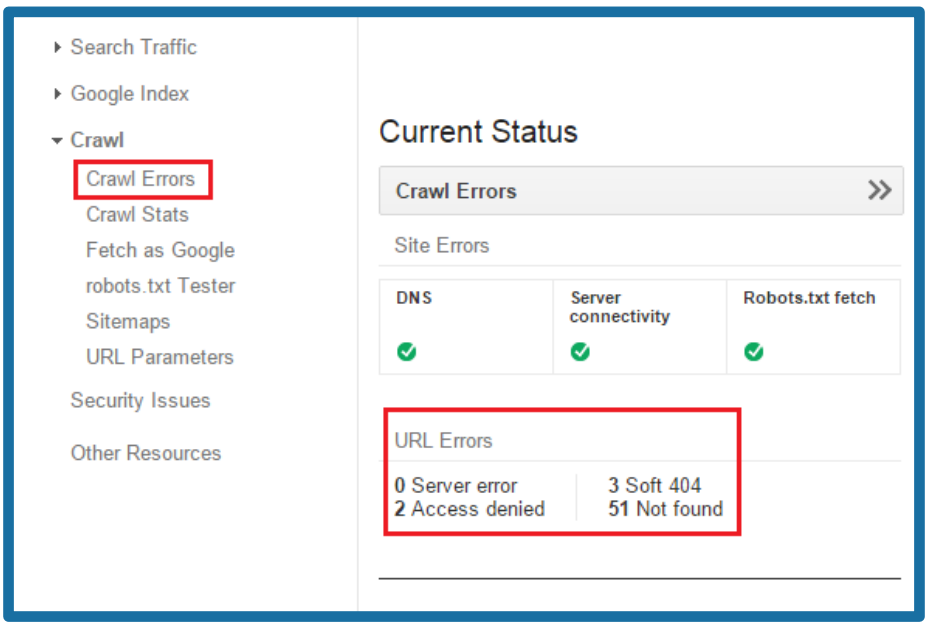


To find existing broken links, you can use a free tool like Xenu Link Sleuth to scan your website.

There are plugins that will do this for you, but they consume a lot of resources which can cause issues especially if you're using a shared web host.

Note: when using the Redirection plugin, be sure to disable log errors in the settings. This will reduce additional server load.

An alternative method of finding 404 errors is to use the crawl error tool within Google Webmaster Tools. Going to the crawl error menu will show you how many 404 errors have been picked up, from there you can find exactly which URL's are broken and which pages are linking to them.



For further reading you can take a look at our tutorial on adding redirects in WordPress.

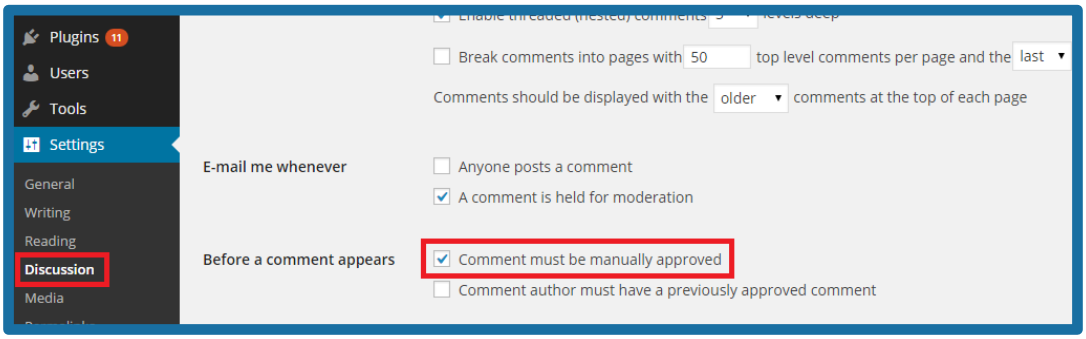
#6. Spam comments are slipping through

If you are using WordPress's blogging functionality, comments are a great signal that people are reading your content but the reality is that most comments are spam.

Some will be obvious; others will be disguised as well written comments for the purpose of promoting another website.

If you let too many spam comments through it can hurt your reputation and count as a negative quality signal when visitors read your comments.

By default, comments are automatically published so you first need to head to your discussion settings and select the option to manually approve comments.



Now that your comments are set to be manually approved, you need to install a plugin to help you deal with the spam – otherwise it will be difficult to manage.

There are plugins that will add captcha's but the reality is that spammers have tools to get around these so the only people you'll alienate will be your legitimate commenters.

There are a few plugins that can work well:

- Akismet – this comes pre-loaded with WordPress, it's an automated tool which can stop a significant amount of spam comments but the downside is that if it picks up legit comments as spam accidently then you will never know.

- G.A.S.P – this plugin combats spam in a few different ways. Firstly, it adds a checkbox which is a lot less annoying for legit commenters than a captcha box. Secondly, it adds hidden fields that only bots can see, this tricks them into filling in the box which helps the plugin identify comment spam.

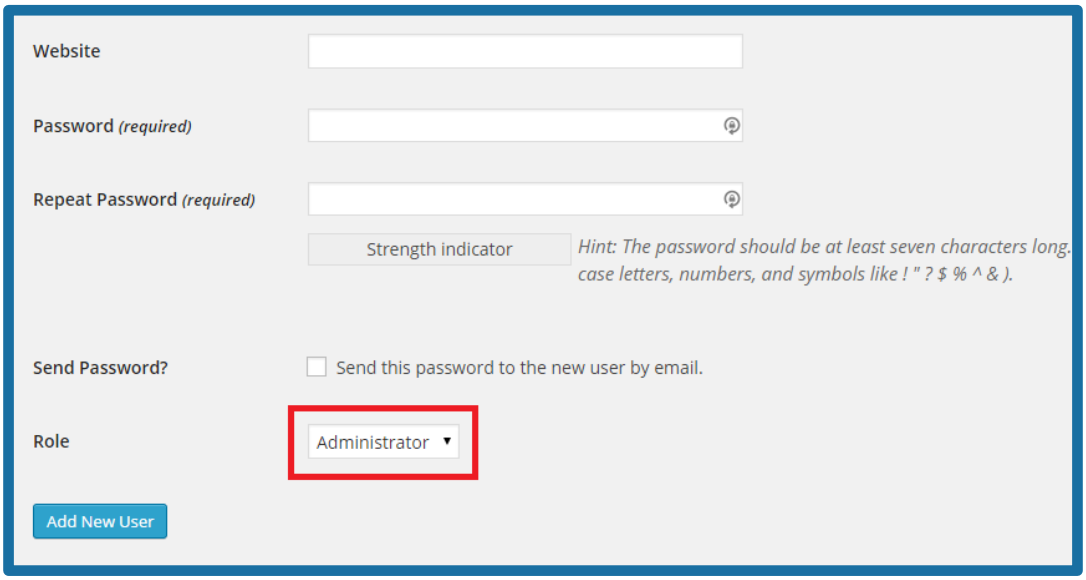
#7. You're still using "admin" as your username

One of the biggest security mistakes is to have “admin” as your username.

Some hackers will use bots that try to access your website by guessing your login details, generally they will use the “admin” username as it’s the most common, so by changing the username you will stop most “brute force” hack attempts.

Most web hosts have one click installers that give you the option to setup your user account with something other than “admin” but there are still those that don’t.

The easiest way to change the username is to actually create a new admin account by going to USERS > ADD NEW.



You then need to make sure the role is set to administrator and to save your new login details (we recommend using LastPass.com to store passwords).

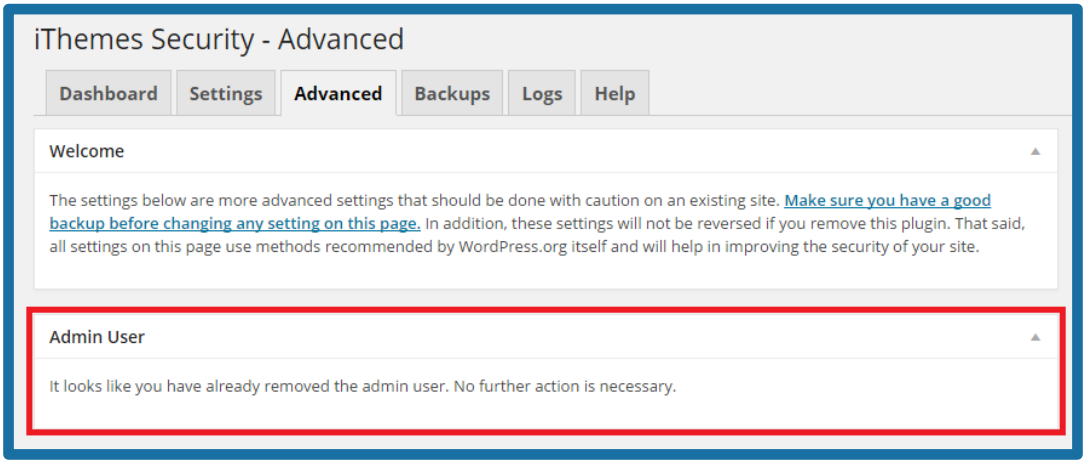
Then you will log out of WordPress, login with the new details and go to USERS > PROFILES then delete the old account with “admin” as the username.

IMPORTANT: Only delete your old account when you have recorded your login details and double checked your new account, otherwise you will be locked out of your website. It’s also worth taking a backup before making any changes.

If you are uncomfortable making these changes, you could use a plugin which would manually change your username for you.

A free security plugin like iThemes Security would do this for you.

Once the plugin is installed, go to SECURITY > ADVANCED and you should see the option near the top.



#8. You’re using weak passwords

If you are using a password that is easy to guess, you are putting your website at risk.

The alternative is to use a tool to generate more complex passwords for you.

Tools like LastPass.com have this functionality built in (it's great for saving passwords too) but you can also use a tool like StrongPasswordGenerator.com to quickly generate a new password that will be more difficult to guess.

An example of a weak password: *Ilovefootball*

An example of a fairly weak password: *Ilovefootball101*

An example of a strong password: *gQ^6zo=jo%Bk&pq*

Why is this such a big deal?

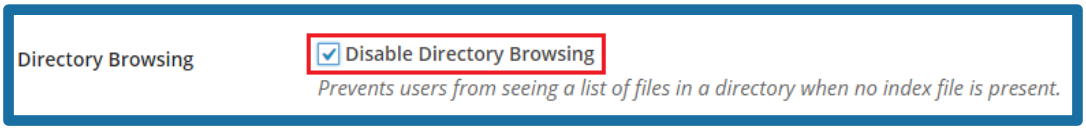
There are lists of the most common passwords that hackers can find on the web. They then use these lists and a bot to conduct "brute force" attacks on various sites so if your password happens to be on those lists, you could have an issue.

#9. You haven’t disabled directory browsing

By default most WordPress installations allow anyone to browse particular directory folders and the files inside them (e.g. your WordPress plugin folder) – this is a big security issue.

To solve this issue, all you need to do is to disable directory browsing.

If you have the iThemes Security plugin installed, this can be done by going to SECURITY > SETTINGS > SYSTSTEM TWEAKS and disabling directory browsing.



You can do this manually by editing the .htaccess file which sits in your root folder. To do this you'll need your FTP logins (your host will provide these for you) and an FTP client (we use FileZilla).

You then need to add the following line to your .htaccess folder:

Options All -Indexes

You can check out our full tutorial here but if you aren't comfortable with editing code, we recommend that you use the iThemes Security plugin to make the change. Alternatively, hire a developer to make the change for you.

#10. You're using the default permalink settings

Permalinks are just the URL's of the posts/pages that you publish using WordPress.

They enable you to structure your content but the default setting isn't very descriptive which in turn can be an issue for your visitors and search engines.

By going to SETTINGS > PERMALINKS within your WordPress admin area you will get the option to change this structure. We typically use the "post name" option.

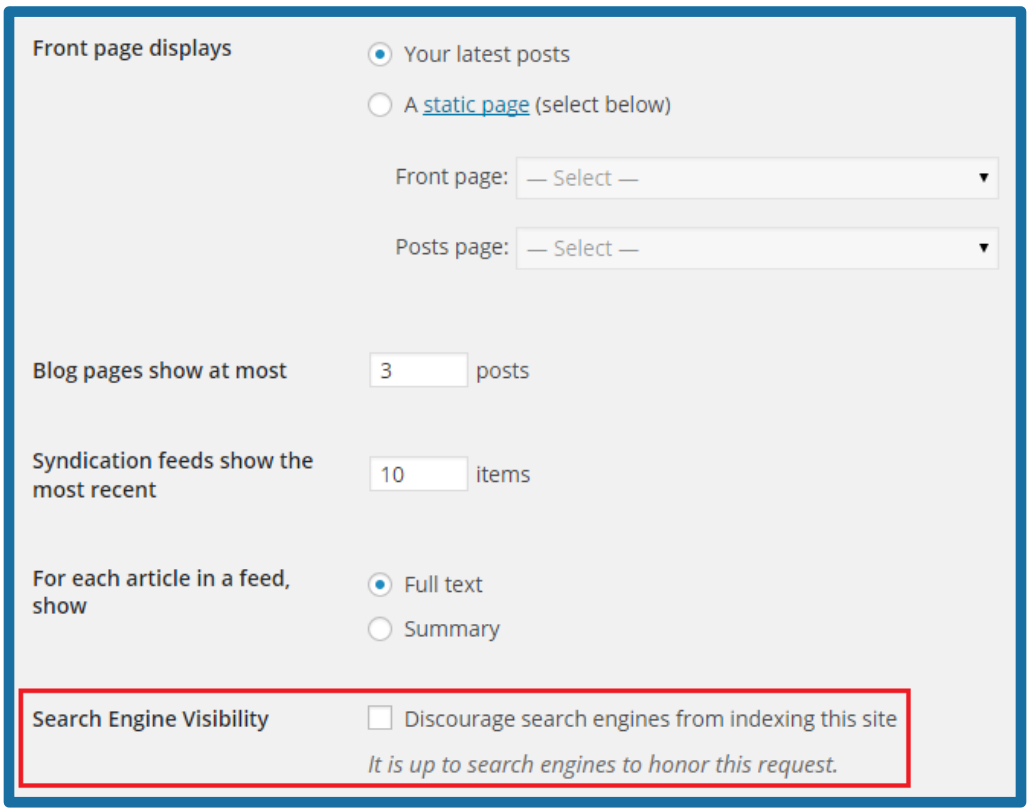
#11. You've accidently blocked search engines

If you're not familiar with WordPress yet, the discourage search engines setting can be easy to overlook.

A lot of developers will select the "discourage search engines" option within the WordPress settings if they want to hide a website from search engines. This is usually done during the development process but some people forget to deselect the option and allow search engines to index their website.

It's an extremely quick fix.

Just head to your WordPress admin area and go to SETTINGS > READING SETTINGS and you'll notice a "discourage search engines" option. You must ensure that this box is NOT ticked.



Conclusion

We've covered some of the biggest mistakes that anyone can make with WordPress and exactly what you need to do to fix them.

You don't have to be a developer to fix any of these but the learning experience of implementing these changes is important. It will help you become more comfortable with WordPress in the future.

Start off by opening up your website and working through this list, ticking off each point as you go along.

Disclosure: *there are a few affiliate links within this guide. This won't cost you anything extra but we might receive a small commission if you make a purchase. This helps to support our team of writers, so we can continue to publish helpful tutorials.*

Get our latest WordPress guides & tutorials from WPSuperstars.net

Start Reading

WP SUPERSTARS
WORDPRESS. SIMPLIFIED.