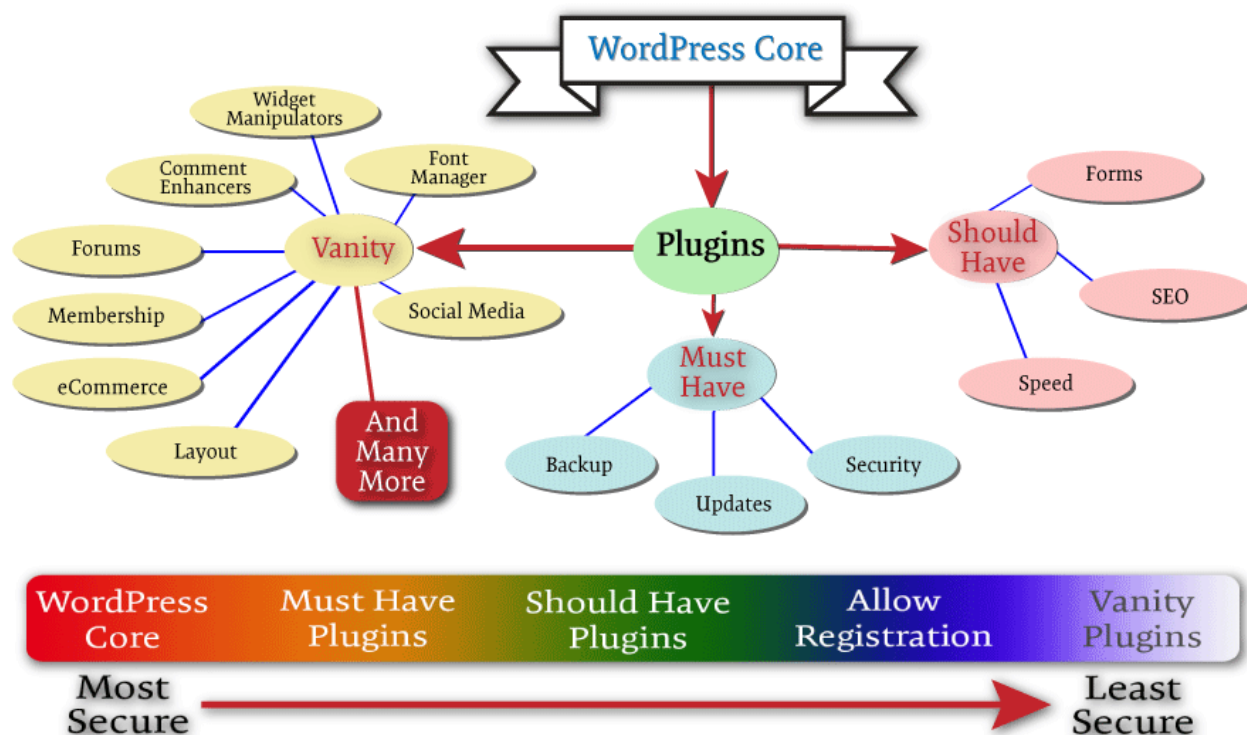# Types of WordPress Plugins I Should Use

WordPress plugins tree

As you can see from the above chart, it is more like the family tree of plugins off the main WordPress core. The explanation and the presentation of it is my interpretation of the WordPress plugin hierarchy. I know some of you may not agree, some of you will, and even more of you will think it is over simplified, but that's the kind of thing I meant to convey.

The WordPress core itself is extremely secure, and by that I mean as secure as any content management system, CMS out there can be. Since it is written and updated by developers, and has a whole community behind it helping its validity, it is one of the most secure CMS's out there today. It has checks and balances because if it.

The WordPress core, (red,) is the most secure version of your site. As it moves to the right and you keep adding more and more things, such as plugins, it gets less secure, (white.) Coming off of the green into the blue area denotes a

website that is more vulnerable to breaking and/ or getting hacked. My best advice is to make sure security is in place, and research your vanity plugins thoroughly before installing them.

Must have plug-ins: These are the plugins in my book that I feel no WordPress website should be without. This will definitely vary from person to person, and from developer to developer. These are the plugins that I recommend, and I am totally open to this changing as I learn more or hear better arguments. That can happen a lot in this business, and one of the coolest thing about WordPress. In this area I have the following categories: **Backups, Updating, Security, and Anti-spam.**

Should have WordPress plugins: These are the plugins that you will install after you have finished installing and testing the plugins on the "Must have" list. This section, plus the previous section will give you a fully functioning interactive site, with the bare minimum of headache when you are trying to keep your site secure. I have included the following categories in this area: **SEO, Caching, Responsiveness, and Forms.** Personally I don't think you can do without any of the plug-ins from either of the above areas. This, to me, is a full site if you are looking to have a functional, interactive site, that also has the chance to be discovered in the web.

Vanity WordPress plugins: Believe it or not, this is a favourite section of mine. I do like my Vanity plugins, because some of them are really cool, add value, and most are very well supported. I am not one of those developer that will poo-poo you because you want to add vanity plugins to your website. If I am designing your website you just have to abide by my rules when it comes to any plugins in this category. You just have to be careful how you choose a Vanity plugin, and what purpose it is supposed to serve on your site.

I have created a table for you to look at with specific examples of plugins I use that fall into each of the areas. Also when adding a new plugin directly from the list below, I have outlined the procedure below, and this procedure should work most of the time, but otherwise it is very easy to figure out:

1. Click the link to the plugin
2. Download the plugin to your hard-drive
3. Go back into your "Admin" section of your site

4. Select "Plugins"
5. Select "Add New"
6. Select "Upload Plugin" at the top of the page
7. Cling the "Choose file" button
8. Find the plugin on your heard-drive – highlight file and select Open, (usually in your downloads folder.)
9. Click the "Install Now"
10. Activate plugin
11. Re-read documentation on the plugin to know how it sets itself up on your computer
12. Check that plugin is there and configure it

Video coming soon on how to download and install a plugin

Area	Category	Specific plugin (* = Best in my book)
Must Have	**Backup**	Backup Buddy * No free version BackWPUp * – Free
	Updating	iThemes Sync * Free – on-line service JetPack Monitor Free – on-line service ManageWP * Monthly subscription – on-line service
	Security	iThemes Security * Free and paid version Sucuri * No free version – on-line CloudFlare * Free and paid version – on-line service Really Simple CAPTCHA – Free
	Anti-Spam	Akismet – * Free and comes with WordPress
Should Have	**SEO**	WordPress SEO by Yoast * Free and paid version
	Caching	W3 Total Cache * – Free and paid version P3 (Plugin Performance Profiler) – Free
	Responsiveness	WP Touch * – Paid version JetPack Mobile theme – Free
	Forms	Gravity Forms * – No free version Contact Forms 7 * Free
Vanity	**Editor**	WPEdit * Free
	Social buttons	Floating Social Bar * Free SumoMe – Free and paid version – On-line service with plugin

Area	Category	Specific plugin (* = Best in my book)
	Widgets	Display Widgets – Free
	Media Library	Enhanced Media Library – Free
	Typogrphy	Google Font Manager – Free Hide Title – Free No Page Comment – Free Yet Another Related Posts Plugin – Free

There are definitely tons more plugins than this, but this will give you a basic idea of the areas that you will most likely need to fill first. Whatever you are looking for can be found by following the steps above the table for finding a plugin or a type of plugin. Let's say you have an idea and you want to see if there is a plugin exists that might help, then type it in.

Remember that a bad plugin has the potential of crashing your site. So when you install a plugin, always check that your site is working after **EACH** install. Don't install 5 or 6 plugins, and then check your site. If it isn't working, then there is no way to tell which plugin was responsible. So take your time and test, test, test as much as you can. Try and limit the number of plugins you install, and delete the plugins that you are not using. Also delete any themes that you aren't using as well. This can help the possible chances that a hacker can get to your website, but all of this is discussed in another article with this site, when I talk about how to tighten up, or lock down your site.

Ten things I do

These are the ten things that I do when I initially start on a clients website. These can vary and some other thing may be done depending on the scope of the project. Most of these are must haves, and others are dependent on the clients needs. But number 10 is a must and happens on every build. Have fun.

1. Change admin user name to something else
2. Install iThemes Security. Run Scan and set it up
3. Delete unused plugins and themes

4. Install W3 Total Cache, and configure it.
5. Install a good backup plugin like BackUp Buddy by or BackWPup, and back up the website.
6. Change permalinks, and other aspects of the settings tab.
7. Make sure the theme, and the plugins I use are well supported.
8. Delete all default pages, posts, and comments
9. Install SEO by Yoast – if client wants search engine work
10. Make some tea or coffee.

This is not all I do, but I make sure these 10 things are definitely done.

Securing your WordPress website

I thought this article was going to be a little further down the line, but something happened yesterday that pushed the timeline up a month or 2. I was working vigorously on getting BarbApple studios up to speed, you know the drill: website with matching Fackbook, and Twitter page, when the unthinkable happened. My servers went down, and the explanation I got was "Our server thought there was too much activity on my site, logging in and out, branded it as malicious activity and we shut you down." This might not have been an issue, but I tried to log in like 7 times, and they couldn't figure out what the issue was.

WordPress was allowing me to change the admin password, but not allowing me to log in. After a day of this nonsense, and back and forth with tech support, it hit us both at the same time. I had a plug installed by BWS plugins called 'Limit Attempts,' and that's what kept me logged out. So when the servers came back online, I was blacklisted from my work computer, and the tech that was helping me also got blacklisted. We went about it 2 different ways, and got the same result, we were able to log back in again.

I had the idea of going to phpmyadmin **and deleting the records** in the plugin table, but thought that was a bit rash, so instead I FTP'd to my site and just deleted the plugins folder. That might be considered rash anyway, although at the same time my tech deleted the records from the database using phpmyadmin. I

don't know which had the desired effect or both, had the desired effect, but I am back. I think his method might have worked fine, but I'd like to think I would have gotten a plugin missing error, and would be allowed in anyway, as this has happened before. So there you are, the beginning of a post on how to secure your WordPress website. This will be part 1) of 2) I think, because I want to do this properly. I am going to discuss the types of things you need to stop, how to stop them, and the reputable plugins that will help. So stay tuned.

WordPress will not crash your website, but plugins and themes will. WordPress, as I have said before, is one of the most stable web environments out there at the moment. When people complain about WordPress crashing, what they usually mean is that it had crashed due to a plugin being bad or in need of updating, or a theme that stopped working. WordPress itself is as stable as it gets on the world wide web.

<p style="text-align:center; color:red;">**BACK UP YOUR SITE!**</p>

This is the most important thing I can tell you to do. Do not assume that the place you are hosting has it covered. Whilst they may do, they could charge you extra money for a restore, and they may not get the restore exactly as you want it. Do it yourself, because WordPress has made it so simple. There are many plugins that will do the job adequately, but the one that I use for all my sites is the plugin BackWPup by Pento. It has been around forever and just does what it says it is going to do. So check that out in the plugins section of my blog, as it is one of my favorites.

Administrator Log in

Do not use admin, user, test**, or administrator** as the main log in user name. When you think about it, they aren't really user names. These are the first names a hacker will attack, and it means that all they have to get now is the password.

Longer passwords are better: You don't have to produce intricate passwords, but long ones – like sentences. People think they have to have longer cryptic passwords, but they forget them. Longer is better in this case, and the chances that you remember it will be better.

If you are the administrator of your WordPress site, create another user account with editor privileges to post to your own blog, so that you are not always

logging in as an administrator. This way there is less of a chance of being key-logged when you are using your website. The admin account you set up should be used for admin purposes only, and this is a good thing to teach your clients also because there is more of a chance of them just posting to their sites than administering to it. This is a tricky one for me because I admin so many sites, that I am admining more than actually posting but your average client will not.

Update your WordPress

Always update your WordPress core, plugins, and your themes whenever they are due. Don't wait a few weeks or even days to do this. The need updated for a reason, so go ahead and do it. You will only make things worse if you don't. Sometimes after I update the WordPress core, I log out and relog back in again to see if anything else has changed in the update department, such as plugins or themes. This may not be necessary, but it is a habit I have gotten into over the years. I just know that I have left updates for a while and crashed my website a few times. There was one time I remember I had to do a full re-install because I didn't update.