oinkodomeo
aircover for sales

WordPress Security Checklist

Here are some things any site owner can do to secure their WordPress website. Don't worry, the items on this checklist require little or no technical knowledge. Once you have done your basic clean up, there are only a few simple tasks that need to be done periodically to maintain the security of your site. Let's started now!

Things to do right away

Manage Users

Many site owners ignore their users but securing your user base is the most important thing you can do to secure your website. Insecure or poorly protected passwords are the single biggest causes of security breach for any website, not just WordPress-based ones.

To start, log into your website with admin privileges and in the sidebar menu click Users->All Users. To see the menu choices for each user, run the cursor over a user's name, the choices will pop up under each name. Do the following:

	Change your admin password. You may be sharing the main admin account with the agency that developed the site. Now is the time to lock them out; you can let them back in later with a new user account if needed. If they have a separate user account, delete it unless you know you will be doing follow-on business with them.
	If you will be contributing content, create a separate account for yourself at the Editor level. Never blog as admin, you are giving away the user name of an admin account, making it easier for a brute force attack.
	Delete any user you do not recognize.
	Review privileges for each user and demote any admin users to Editor if they don't need admin access. You should have no more than three admin users.
	Publish a password policy and enforce it. The most important rules are; do not share passwords, keep a strong password (at least 7 characters, upper/lower case, one symbol, one number). The WordPress password monitor should give your password at least a medium rating.

General Settings

	On the general settings page, ensure that the contact address is one you monitor daily. WordPress will send update alerts to this address.
	Ensure that new user default role is set to Subscriber. You will need to upgrade a user to a higher level of privilege when you create the user.
	Make sure the time zone is set correctly for your time zone. This will be useful when you set up backups.

Plugins for Security

Install and activate both of these plugins from the WordPress Plugin Repository.

From the dashboard sidebar menu select Plugins->Add New, then search on the plugins name. That way you ensure that you are getting the genuine plugin.

	Install Wordfence or a similar security plugin. The free version of Wordfence includes protection from brute force attacks, malware scanning and an application firewall. It remains one of our top five favorite plugins. Wordfence does most of its own setup on activation, so you don't have to worry about it much, but there are multiple articles available online for configuring Wordfence (just be sure you have a current one).
	Install backup software. We like Updraft Plus. Arrange for third party backup storage and write out a backup to that storage at least once a week, during down time for your site. Keep the last five backups, but remember these cost you disk space on your web server.

General Plugins

Plugins can be difficult to manage, as many are installed during development and then not used. Sometimes several plugins that perform similar functions are installed, but only one is used; the rest are left de-activated. You can generally tell what a plugin does from its description, but it is not always clear where it is implemented on the site. The good new is, you can generally re-instate a plugin you deleted by mistake (be sure you log its name before you delete it). Also, unless a plugin is very unstable or insecure, you can usually de-activate it for a week or two, and if you don't see anything broken, you can delete it.

Here is what to do now. In your dashboard, go to Dashboard->Updates.

	For the list of plugins that need to be updated, select all, then update plugins. **Watch the alerts that go by, and make a note of any plugins that do not update completely.**

Now go to Plugins->Installed Plugins:

	Delete any plugins that are currently de-activated
	De-activate any plugins that did not update properly in the procedure above

A full plugin audit is beyond the scope of this checklist (We'll provide a boilerplate audit procedure soon).

Administrative Stuff

The items in this section will be very important if your site is ever hacked. Too often significant time is wasted identifying the web host, domain registrar and other responsible parties while the crisis is occurring.

To avoid this, do the following:

	Identify the Internet Service Provider (ISP) or other entity who is hosting your website. If the host is the digital agency that your company parted ways with, you may need to find a new host and migrate your site to them. Understand and document how to contact your ISP, and how to open a service ticket with them, as well as how to get emergency service if you need it.
	Ensure that you can log into any service or control panel your host provides, whether or not you understand any of the functions
	Determine if your web host is also handling your company email, and if not, who is, and what is their contact information
	Identify the domain registrar for your domain (GoDaddy or similar). Ensure that you have the login credentials for the domain, and the date your domain must be renewed.
	Identify at least one other employee to hold an admin account who is trained on basic procedures, including user management
	Setup priority communication between Human Resources, you, and your alternate in case a user's access needs revoked
	Start a log book that you keep in a secure location. The first few pages should be reserved for contacts, including top management, human resources, the hosting provider ISP, the domain registrar, your contact in company IT, and your digital agency if you have one. The next several pages are for relevant access codes and your admin password log, because you will be changing your password every six months. In subsequent pages, write down and date stamp everything significant such as major updates, plugins added, plugins deleted, new users, anything of significance that happened, when it happened and why it happened. Log specific details.
	Ensure that your alternate has an up to date list of the important contacts you have gathered

Congratulations, you have completed the hard part!

Now there are just a few simple tasks to do on a regular basis.

Things to do weekly

As a practice, this may be the only time you log in as admin. Check your analytics, and set aside ½ hour every week during down time when there are few visitors. Log in as admin and do the following:

	Ensure that your backup completed normally, and wrote the backup to third party storage
	Update plugins, log any issues you see during update
	If a WordPress version update is available, take the update. Check your site for basic function and display.
	Update themes (Note: keep one of the WordPress default themes you can test with. Other themes that are not default should be deleted)
	Check your security plugin for any alerts such as excessive login attempts etc.

Things to do monthly

	Check analytics for anything unusual, such as abnormal traffic from a country overseas or a less popular browser
	Download a full backup to fixed media such as a USB disk or drive

Things to do every six months

	You and your admin alternate should change your passwords
	Re-check all of your contact info and logins to see that they are still valid
	Review any changes your ISP has made to the service they offer, particularly technical support, which is often outsourced overseas. To be truthful we have had some excellent experiences with overseas tech support, but it is best to be aware
	Review your users. Remove anyone who no longer needs access.
	Send a reminder to current users that they should change their passwords, and not share their passwords with anyone
	Conduct a plugin audit. We will publish a boilerplate procedure for this in the coming weeks.

Want to learn more or need help? Contact us at Oinkodomeo.