Your crash course in WordPress security

The security of your website is exceptionally important. WordPress powers 26% of all websites and that doesn't make it vulnerable per se, but makes it a target.

WordPress is not impenetrable, but it's safe to assume the latest version is secure and any vulnerabilities that do exist will be fixed with updates within hours or days.

This means **the best way to keep your site secure is to make sure your WordPress installation is always up-to-date**.

Plugins and themes are a separate issue; there's not the same level of vigilance regarding their security and updates may be slower. The best practice is still to keep everything up-to-date all the time, but if a theme or plugin isn't updated to cover security vulnerabilities, having the latest version of an insecure theme or plugin is of little help.

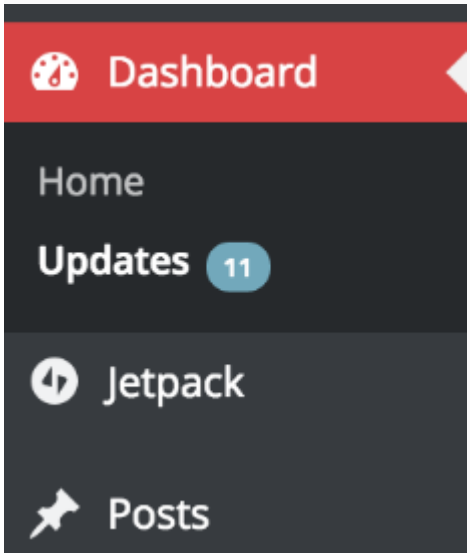
The *better* practice, therefore, is to only use themes and plugins you can reasonably assume will be continually updated. A good rule of thumb is check when the last update was. If it's more than 6-12 months old, that's generally an indicator of infrequent updates. If the last update is more than 18-24 months ago, the plugin has likely been abandoned and should be avoided (although well-made plugins with simple functionality can be "old" but safe). If you're using a premium theme without automatic updates make sure you're signed up for notifications of available updates.

> NB: A particular problem to be aware of is themes bundling plugins. Themes recommending you separately install plugins is fine, the dangerous thing is themes including plugins in their code. This means you can't get updates for the plugin without updating the entire theme – and it's unlikely there'll be a new version of the theme for every single release of the plugin.
>
> The danger of this was highlighted by a critical vulnerability showing up in a plugin that was frequently bundled with themes on ThemeForest. The plugin needed updating to fix the problem. Three months later, over 100,000 sites were yet to be updated, with over 11,000 of those attacked.

Security is something to take very seriously. Keeping everything up-to-date is the basic requirement here. We'll run you through how to do this, common issues you'll run into and how to automate the entire process.

Updating WordPress, themes and plugins

WordPress makes it very easy to update your installation, themes and plugins all from one place. If any updates are available, a number will show on the WordPress Dashboard menu, as you'll see below:



Click through and you'll be able to see what can be updated. WordPress will automatically update minor releases of WordPress itself and themes and plugins in exceptional circumstances (if the WordPress.org team regards an update as necessary to fix a known security vulnerbility). This means there'll likely be some updates to do. We'll cover how to make everything automatic later but walk you through manual updates first.

Before you update anything you'll be warned you need to do a backup first. This is true, but it's a pain to do and it's one of those things everybody knows they should do but doesn't. Instead of doing ad-hoc backups every time you do updates, it's better to have reliable automatic backups at a frequency that makes sense for however often you update your site (if you have frequent updates, once a day is good – infrequent, fortnightly or monthly is fine).

You can update WordPress by pressing "Update Now". For themes and plugins you'll want to tick "Select All" and then update. WordPress will handle the update and there shouldn't be any issues.

Troubleshooting common issues

There are two issues you'll likely come across:

1. Stuck in maintenance mode

When you run an update WordPress puts your site into “maintenance mode”. If for whatever reason the backup won't complete your site will be stuck in this mode, complete with the homepage being replaced with a message stating “Briefly unavailable for scheduled maintenance”.

Not pretty.

This is easy to fix. Log in to the root of your site via FTP and you’ll find a new file: .maintenance. Delete this file and you’ll get your site back. You can then run the update again and it usually works a second time.

2. Automatic updates not happening

The second common issue is automatic updates don’t happen. If you’re using a “managed” WordPress host that handles things like updates for you, this would explain it. Your host may just take a short time to check the new version for any bugs or issues and then apply the update a short time later. Contact support if there’s any serious delay.

If you’re expecting automatic updates that just aren’t happening then install the Background Update Testerplugin. This will tell you what’s not working and why, with steps to fix it. Your host’s support will likely be able to help you out here (especially if they offer “WordPress compatibility”, which most hosts will).

Another possible cause of automatic updates not happening is if WordPress detects you are using Git or Svn to manage your website. Since these are quite technical things, WordPress assumes that people using them will update their site when required. If you’re using a version control system then make sure you update your local version and deploy to your website.

Automating updates

Manual updates are fine, but a WordPress Master prefers to automate what doesn't need to be done manually. WordPress can do this for you (and we'll get to that), but there's an option that's easier to set up and scales a lot faster (so better if you're dealing with lots of sites).

Using ManageWP

ManageWP is one of many WordPress management platforms but its free account offers much more than the competition, including automatic updates and once-a-month cloud backups (NB ManageWP has recently been bought by GoDaddy, but they say the free accounts are here to stay for now).

They recently released a new dashboard, Orion, which is generally much easier to use, but tragically gets rid of the automatic updates feature seen in the old version. You used to be able to set-and-forget ManageWP to handle all updates across all your sites, but no more. I'm told it is a feature that's coming back, but there's no ETA at present.

It's worth having ManageWP installed anyway to keep an eye on your sites, and hopefully it'll soon again be the one-stop solution to site updates. In the meantime, we're in need a new solution to get updates done automatically.

Getting WordPress to update for you

In the meantime, WordPress has you covered. Built-in automatic updates is a little known but extremely useful feature.

To set this up you'll need to access your site using an FTP editor, navigate to the root of your WordPress installation (probably yoursite.com/) and edit the file`wp-config.php`. Add the lines:

```
define( 'WP_AUTO_UPDATE_CORE', true );
add_filter( 'auto_update_plugin', '__return_true' );
add_filter( 'auto_update_theme', '__return_true' );
```

Update the file and you're done.

For `WP_AUTO_UPDATE_CORE` you can change `true` to`false` to disable automatic updates entirely (not recommended but if you need to test everything first and will update manually promptly could be necessary) or change to `minor` to enable automatic updates for minor releases but not major releases (this is what happens by default).

You'll need to do this on every site you want automatic updates on. It'd be easier to use ManageWP on all your sites, but whilst there are no automatic updates available this is the best option.

Hardening WordPress security

You can keep WordPress secure by protecting yourself from widespread vulnerabilities in the software itself but you may still be vulnerable to weaknesses from users, plugins and themes. There are a number of things you can do to lock down the rest of your site.

Take advantage of Jetpack's security features

The ever-useful Jetpack plugin features some useful security features. You'll find these under Jetpack → Settings → Security. The essential feature to activate is Protect, which will prevent brute-force login attempts by locking out users with large number of wrong password entries. You can enter your IP address so you're not accidentally locked out your own site.

You can also make use of Jetpack's downtime monitoring so you know when something's up with your site. Security scanning is also available as a pro feature.

Use strong passwords and two factor authentication.

WordPress will warn you when creating a password if it's weak, but you'll get an even stronger password using a password manager such as 1Password orLastPass will get you an even stronger password (which, with a password manager, you don't need to specifically remember).

You'll then want to pair your strong password with two factor authentication, so even if someone has your password, only you can login as you'll need a code from your phone. Google Authenticator is a free plugin which lets you use Google's secure app (which you may already have) to logon to your site. Installation is easy and adds a strong extra security layer to your site.

Lock down the plugin and theme editor

The little-loved `wp-config.php` file is probably the most important file in your WordPress installation. Without it, WordPress is missing basic configuration details and can't connect with your database.

If you use an automatic installation service for your WordPress install you'll find `wp-config.php` handled for you. Otherwise, you'll need to enter your details to`wp-config-sample.php` and rename the file once you're done.

Normally the config file is touched when doing the famous five minute install and at not at any other time. This is sad, because it lets you enable some really handy security features. Load up the file for editing and add the following two lines:

```
define( 'DISALLOW_FILE_EDIT', true );
define( 'DISALLOW_FILE_MODS', true );
```

This will tell WordPress to disable the plugin and theme editor, and disable the plugin and theme installer and updater respectively. Using these will prevent users (or clients) from interfering and making any changes which may compromise your site. Good to know.

Because wp-config is such a powerful file, always be extra careful when editing (and create a backup of the file). Here's what WordPress.org recommends:

Before you save the file, be sure to double-check that you have not accidentally deleted any of the single quotes around the parameter values. Be sure there is nothing after the closing PHP tag in the file. The last thing in the file should be ?> and nothing else. No spaces.

So – double check and then save. Enjoy the added safety.

Be careful with themes and plugins

Themes and plugins aren't dangerous per se, but as they're allowing code from an unknown source to run on your site you need to know you can trust them. Two easy rules to follow:

1. **Only install themes and plugins from reputable sources.** That means the WordPress theme and plugin repositories and well-established third-party premium sources. Avoid sites offering free versions of premium themes.
2. **Keep plugins to a minimum and delete plugins that are no longer needed.** The more plugins you have, the more likely there will be a security vulnerability on your site. Deactivate and delete those you're not using any more.

Keep an eye on users and permissions

You can have all the security in the world, but if you give the key to the wrong person it's not going to help. Make sure users only have the level of permission they need: be especially careful handing out administrator accounts, and keep an eye on who can publish content without you knowing (editor and author roles). Also make sure user registration is disabled (provided it's not needed), so you have control over which accounts exist.

If you need help from theme or plugin support create a temporary user rather than creating a new user, use this plugin to create a temporary login which can expire after a couple of days. After you're done with support, the account can be deactivated and there's no risk of continued access.

Security is important

Security is really not something to take lightly. WordPress generally gives you nothing to worry about – but only if you're always up-to-date. This lesson has given you the skills you need to handle WordPress' updates and the tools you need to automate the process. You're even equipped if anything goes wrong :)

This is something to set-and-forget, and something to set right now – so get to it!