WordPress Security

As the operators of WordPress.com, the biggest WordPress site on the web, we know all the secrets, tips, and tricks to help WordPress shine at scale. We're a global company dedicated to making WordPress work better for our clients and users. In this document we share common WordPress security questions and best practices.

Is WordPress secure for Fortune 500 companies' websites?

Definitely. We count many of them among our list of VIP clients, and many others use WordPress on their own servers. vip.wordpress.com/clients/ lists some of our clients and vip.wordpress.com/spotlight/fortune-500 also introduces some enterprises and companies in the Fortune 500 using WordPress in various ways.

Is WordPress safe for government agencies and other public-facing sites?

Absolutely! In fact, a whole slew of government sites are already using WordPress. Check out our Spotlight on WordPress for Government (vip.wordpress.com/government) for more information and examples. NASA, the U.S. Senate Democrats, and the Republican and Democratic party websites all run on WordPress.

What happens when there's a security problem in WordPress core software?

If a critical security vulnerability is identified in WordPress, the goal is to issue a security release that addresses it as quickly as possible (typically within days, but often faster) depending on the severity and complexity of the issue.

I've heard of X WordPress site being hacked — can it happen to my WordPress site?

WordPress.com VIP has had a lot of experience helping clients with "hacked" sites and though each case is different, two types of "hacks" unrelated to WordPress often receive a lot of attention.

The first case is a weak user password or a user's password being utilized across multiple services, and one of those other services gets compromised. In this case, the password is compromised and used to obtain access to the WordPress site. The site hasn't technically been hacked at the software level; the user's password has been compromised.

We have some strong password guidelines we recommend for all users (which we talk about below) – make sure you keep your user list updated and encourage your users to regularly change and create strong passwords.

The second case is when a hack happens at the file system level of a particular shared web host's server. Since the file system is compromised, files can be modified and Javascript or PHP injections are common and this can affect any software running on the server; Drupal, Joomla, or WordPress! Usually it's something the individual hosting provider can prevent by increasing security on their shared file systems and servers.

If you need some assistance in setting up your servers to be secure, that's something we can help you with via VIP Support: vip.wordpress.com/our-services/#self-hosted

What happens if my team discovers a WordPress security issue?

If you find a security flaw in core WordPress, here are the instructions on WordPress.org about reporting security flaws: codex.wordpress.org/Security_FAQ.

"The WordPress security team is made up of 25 experts including lead developers and security researchers — about half are employees of Automattic, and a number work in the web security field. We consult with well-known and trusted security researchers and hosting companies." — Andrew Nacin, WordPress Lead Developer, in a presentation 'WordPress.org & Optimizing Security for your WordPress sites,' June 2013.

For a WordPress.com security issue, please see the Automattic Security page automattic.com/security.

For a WordPress plugin security issue, email plugins [at] wordpress.org with as much detail as you can. You should also contact the plugin developer either via email (if it's listed in the plugin source code), or by posting in the support forum on their plugin page asking how best to send them details.

For a security issue with the self-hosted version of WordPress, email security [at] wordpress.org with as much detail as you can.

What about X plugin — is it safe?

Plugins aren't as rigorously reviewed as the core software, and there are occasional, wide-spread security issues that they've introduced. We encourage everyone to review any code they're planning to run on their site — and that's also why WordPress.com VIP provides code reviews as a service for our support customers as well. vip.wordpress.com/our-services#self-hosted.

How does WordPress.com VIP Hosting handle DDoS?

At WordPress.com VIP, we have various types of DDoS protections in place as well as various mitigation strategies when they come up. DDoS can happen several times a day but in most cases you won't notice as either they're small and our infrastructure can absorb the increased load, or our automated protections kick in and apply various techniques to minimize the impact.

For extremely large-scale attacks, if we have control over DNS or you're using a CNAME we have other DNS-level mitigation techniques to minimize the impact on the site and others on WordPress.com.

Do your WordPress.com VIP clients ever do security audits to determine whether or not your security setup matches their internal requirements? If so, what does that process look like?

If necessary, and compatible with our own guidelines and requirements, we will work with a security audit team to provide more information about security on WordPress.com VIP.

Strong Password Guidelines

Every password you use has to be easy to remember and hard to guess. A random set of numbers and characters make for a hard-to-guess password, but they're also hard to remember. On the other hand, you'll probably never forget your birthdate or the name of your first pet, but these make for very bad passwords, as they are increasingly easy to guess or research.

On WordPress.com, you can use a very long password with any combination of letters, numbers, and special characters, so the security of your password – and by extension, of your site – is really up to you.

To choose a memorable password that will be hard to guess, come up with a word or two that are not in any dictionary, yet are easy to pronounce. It's easier to remember a pronounceable word then a string of random characters. Then, mix in some numbers, capital letters, or special characters.

You can also use pass-phrases – whole sentences, such as quotes or favorite song lyrics, peppered with some random numbers and special characters. Pass-phrases are harder to guess yet easier to remember. They take longer to type, but are considered more secure.

However, even if you manage to think of a good password, it will only be as secure as the number of sites you use it on. If you always use the same password on every site you sign up for, the chances of your password getting compromised are greatly increased.

Instead of trying to keep track of dozens of passwords in your head or in unsecured text documents on your desktop, use password management software. They will lock all your information down behind one single password. If you only have to remember one password, you can make it as random and as hard to guess as you want.

These are some password managers we recommend:

- Keepass – Open Source, free to download and use. Available for Windows, Mac and Linux.
- LastPass – Free service with premium option. Available for all major OSs, browsers and mobile devices.
- 1Password – Paid download. Available for Windows, Mac and iOS, with support for all major browsers.

Security Best Practices for End-Users

KEEPING YOUR SECRETS SECRET

The weakest link in the security of anything you do online is your password. It's the key to your site, your email, your social networking accounts or any other online service you use. If your password is easy to guess, your online identity is vulnerable.

All it takes is one person to guess your password and they can delete every post you ever made. They could deface your site. They could read you emails or hijack your address and impersonate you. They could ruin what you have taken time to build.

LOGGING OUT TO PREVENT PUBLIC ACCESS TO YOUR DASHBOARD

You can protect your account by logging out when you are finished working. This is especially important when you are working on a shared or public computer. If you don't log out, someone may be able to access your account just by viewing the browser history and going back to your WordPress.com Dashboard.

To log out of your WordPress.com account, select My Account → Log Out from the gray toolbar at the top of any WordPress.com page. Make sure you log out when you're done editing!

ROLES & PERMISSIONS: SAFELY SHARING CONTROL OF YOUR SITE WITH OTHER USERS

WordPress.com provides a rich multi-user platform. While each site has only one owner, you can have as many users as you want – this is ideal for group sites with multiple authors, for magazine-style sites with an editorial workflow, or for any other large site where you want to share some of the administrative load.

However, sharing the load also means sharing the responsibilities. That's why on WordPress.com, you can set different Roles for each user you add to your site. Roles determine a user's access level.

The most limited role, Contributor, can only write draft posts, but can't publish them. Users with an Author role can publish posts and upload images, but can't touch other users' posts. Editors can not only edit or publish any user's posts, they can also moderate comments and manage categories and tags. Finally, the Administrator role has full control of the site – they can even delete it or remove other Administrators.

When adding users, try to find the role that best describes what you want them to do on your site. If you're setting up an account for a user that only plans to contribute a few posts, make them a contributor. Reserve the Author and Editor roles for trusted users that have a long-term commitment to your site.

Finally, be particularly stingy with the Administrator role. When you make another user an Administrator on your site, you're literally creating a separate set of keys for your site and handing them to someone else. Not only will they be able to take your site for a joyride, just having an extra set of keys laying around significantly increases the risk of your site being hijacked. In fact, we suggest you avoid the Administrator role entirely. In almost all cases, the Editor role would be a better choice.

USING A SECURE CONNECTION TO LOG IN TO WORDPRESS.COM

When you sign in to WordPress.com via a public Internet connection, such as a Wi-Fi connection at a library or a coffee shop, your account may be vulnerable to hijacking.

To keep the bad guys out, you can use a secure, encrypted connection to connect to your Dashboard. Under Users → Personal Settings, check the box that says "Always use HTTPS when visiting administration pages, and click Save Changes.

When you log out and log back in, you'll be using a secure, encrypted connection, and on one will be able to decipher your communications with the Dashboard. Note however that this may cause the Dashboard to feel a little slower. To learn more about this options, see the HTTPS support page.

AUGMENT YOUR PASSWORD WITH AN EXTRA LAYER OF AUTHENTICATION

With Two Step Authentication, you can use any iOS, Android, Blackberry, or SMS-capable mobile device as a unique key to your site. After you sign up for the service, you will need to enter a specially generated one-time code whenever you try to log in to your site. This means that even if someone gets your password, they won't be able to log in without possessing your mobile device as well. You can learn more about this service in the Two Step Authentication support page:
en.support.wordpress.com/security/two-step-authentication.

Have a question which hasn't been answered here, or want to get started with WordPress.com VIP Services for your site?

Get in touch!
vip.wordpress.com/contact

OTHER HELPFUL RESOURCES FROM WORDPRESS.COM VIP:

- Enterprise case studies: vip.wordpress.com/category/case-studies
- Why choose WordPress.com VIP? vip.wordpress.com/why-vip
- WordPress.com VIP clients: vip.wordpress.com/clients
- Building WordPress sites for different sectors: vip.wordpress.com/spotlight