



The Ultimate Guide to Securing Client Sites

KINSTA



For the always up to date version scan the
QR code above or go to:

<https://www.kinsta.com/ebooks/>

Published by **KINSTA**

The Ultimate Guide to Securing Client Sites

Contents

6

Invest in Secure
WordPress Hosting

7

Use Latest PHP
Version

10

Use Clever
Usernames and
Passwords

11

Always Use the
Latest Version of
WordPress, Plugins,
and Themes

14

Lock Down Your
WordPress Admin

18

Take Advantage
of Two-Factor
Authentication (2FA)

20

Use HTTPS
for Encrypted
Connections – SSL
Certificate

20

6 Key Reasons Why
HTTPS is important
beyond just
eCommerce

22

Disable XML-RPC

22

Add Latest HTTP
Security Headers

24

Use WordPress
Security Plugins

25

Harden Database
Security

26

Always Use Secure
Connections

27

Check File and Server
Permissions

29

DDoS Protection

30

Always Take
Backups

32

WordPress Backup
Plugins

33

Summary

The Ultimate Guide to Securing Client Sites

According to [internet live stats](#) over 100,000 websites are hacked every day. 😞 That's why it's so important to take some time and go through the following recommendations below on how to better harden your WordPress security.

When it comes to WordPress security, there is much more than just locking down your site, although we'll give you the best recommendations on how to do that below.

Websites hacked today
111,760
All on this page, one by one

Invest in Secure WordPress Hosting

Let's start with web server-level security for which your WordPress host is responsible for. It's very important that you choose a host that you can trust with your business as you move your clients' sites over to them.

If you are hosting WordPress on your own VPS, then you need to have the technical knowledge to do these things yourself. But to be honest, [trying to be a sysadmin to save \\$20/month](#) is not an effective way to run a business.

Server hardening is the key to maintaining a thoroughly-secure WordPress environment. It takes multiple layers of hardware and

software level security measures to ensure the IT infrastructure hosting WordPress sites is capable of defending against sophisticated threats, both physical and virtual.

For this reason, servers hosting WordPress should be updated with the latest operating system and (security) software, as well as thoroughly tested and scanned for vulnerabilities and malware.

Server-level firewalls and intrusion detection systems should also be in place to keep your clients' sites well-protected even during the WordPress installation and website construction phases. However, all software installed on the machine intended to protect WordPress content should be compatible with the latest database management systems to maintain optimal performance. The server should also be configured to use secure networking and file transfer encryption protocols (such as SFTP instead of FTP) to hide away sensitive content from malicious intruders.

We use [Google Cloud Platform](#) here at Kinsta for all of our WordPress customers to ensure [secure WordPress hosting](#). Security is built into our architecture from the beginning and it's a much more safer method than others available today.

Use Latest PHP Version

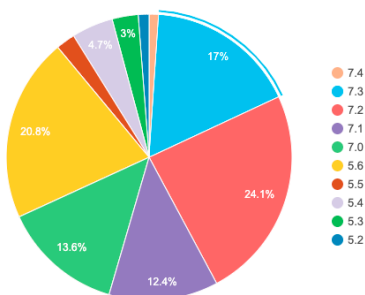
PHP is the backbone of any WordPress site, so making sure your clients' sites are using the latest version on your server is very important. Each major release of PHP is typically fully [supported for two years](#) after its release.

During that time, bugs and security issues are fixed and patched on a regular basis. As of today, anyone running on version PHP 7.1 or below no longer has security support and are exposed to unpatched security vulnerabilities.

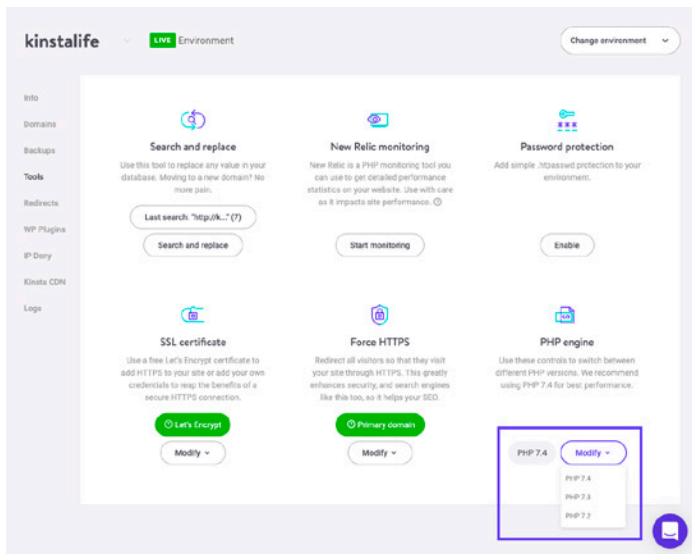


And guess what? According to the official [WordPress Stats](#) page, around 34% of WordPress users are still on PHP 5.6 or lower which means, more than a third of the users are currently using PHP versions that are no longer supported. That is scary!

PHP Versions



Here at Kinsta we only recommend using stable and supported versions of PHP, including 7.2, 7.3, and 7.4. PHP 5.6, 7.0, and 7.1 have been phased out. You can even [switch between PHP versions](#) with a click of a button from within the MyKinsta dashboard.



If you want to try it yourself, just head to demo.kinsta.com and give it a try!



Use Clever Usernames and Passwords

Surprisingly one of the best ways to harden your WordPress security is to simply use clever usernames and passwords. Sounds pretty easy right? Well, check out [SplashData's 2019 annual list](#) of the most popular passwords stolen throughout the year (sorted in order of popularity).

- 123456
- 123456789
- qwerty
- password
- 1234567
- 12345678
- 12345
- iloveyou
- 111111
- 123123

The most popular password is “123456”. That is one reason why here at Kinsta on new WordPress installs we actually force a complex password to be used for any of your clients’ [wp-admin login](#) (as seen below on our one-click install process). This is not optional.

Location

You can choose between 21 data center locations, which allows you to place your website in a geographical location closest to your visitors.

WordPress site title

WordPress admin username

WordPress admin password

WordPress admin email

Select a language

Check out this feature
with the MyKinsta demo.



The core WordPress `wp_hash_password` function uses the [phpass](#) password hashing framework and eight passes of MD5-based hashing. And as far as your WordPress install goes, you should never use the default “admin” username on your clients’ sites, rather create unique WordPress usernames for their administrator accounts.

It is also important to use different passwords for every client site. The best way to store them is locally in an encrypted database on your computer.

A good free tool for this is [KeePass](#). If you don’t want to go down this route there are also online password managers such as [1Password](#) or [LastPass](#).

Always Use the Latest Version of WordPress, Plugins, and Themes

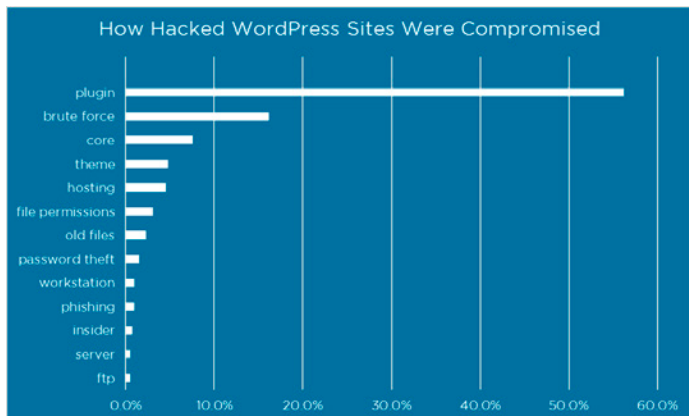
Another very important way to harden the security of your clients’ sites is to always keep them up to date. This includes WordPress core, plugins, and [themes](#). These are updated for a reason, and a lot of times these include security enhancements and bug fixes.

Unfortunately, millions of businesses out there running outdated versions of WordPress software and plugins, and still believe they’re

on the right path of business success. They cite reasons for not updating such as “their site will break” or “core modifications will be gone” or “plugin X won’t work” or “they just don’t need the new functionality”.

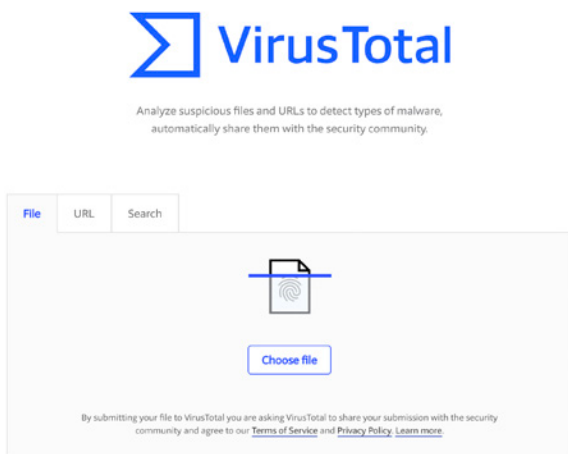
In fact, websites break mostly because of bugs in older WordPress versions. Core modifications are never recommended by the WordPress team and expert developers who understand the risks involved. And WordPress updates mostly include must-have security patches along with the added functionality required to run the latest plugins.

Did you know that it has been reported that [plugin vulnerabilities represent 55.9%](#) of the known entry points for hackers? That is what WordFence found in a study where they interviewed over 1,000 WordPress site owners that had been victims of attacks. By updating your plugins you can better ensure that you aren’t one of these victims.



It is also recommended that you only install trusted plugins for your clients. The “featured” and “popular” categories in the WordPress repository can be a good place to start. Or download it directly from the developer’s website. We strongly discourage any use of [nulled WordPress plugins and themes](#).

You can use an online tool like [VirusTotal](#) to scan a plugin or theme’s files to see if it detects any type of malware.



There are also a lot of resources out there to help you stay on top of the latest WordPress security updates and vulnerabilities. See some of them included below:

- [WP Security Bloggers](#): An awesome aggregated resource of 20+ security feeds.
- [WPScan Vulnerability Database](#): Catalogs over 10,000 WordPress Core, Plugin and Theme vulnerabilities.

- [ThreatPress](#): Daily updated database of WordPress plugins, themes, and WordPress core vulnerabilities.
- [Official WordPress Security Archive](#)

Lock Down Your WordPress Admin

Sometimes the popular strategy of WordPress security by obscurity is appropriately effective for an average online business and WordPress site. If you make it harder for hackers to find certain backdoors then you are less likely to be attacked. [Locking down your clients' WordPress admin area](#) and login is a good way to beef up your security. Two great ways to do this is first by changing your default wp-admin login URL and also limiting login attempts.

How to Change Your WordPress Login URL

By default your WordPress site's login URL is domain.com/wp-admin. One of the problems with this is that all of the bots, hackers, and scripts out there also know this. By changing the URL you can make yourself less of a target and better protect yourself against brute force attacks. This is not a fix-all solution, it is simply one little trick that can definitely help protect you.

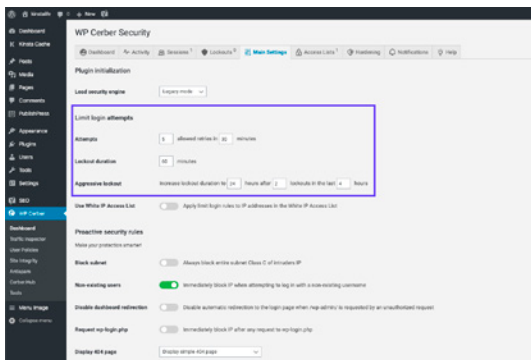


The screenshot shows the WordPress settings page for changing the login URL. It features two input fields: 'Login url' and 'Redirection url'. The 'Login url' field contains 'https://k1nsta13f3.com/new-ur1' and the 'Redirection url' field contains 'https://k1nsta13f3.com/404'. Below each field is a small explanatory text. A 'Save Changes' button is located at the bottom left of the form area.

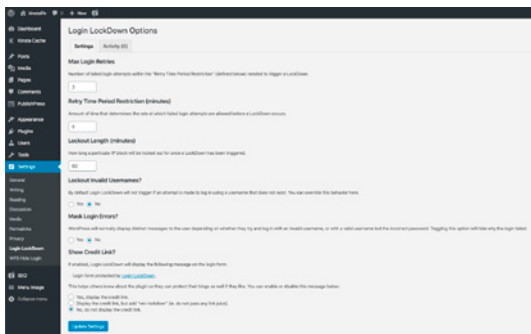
To [change your WordPress login URL](#) we recommend using the free WPS Hide login plugin. Just remember to pick something unique that won't already be on a list that a bot or script might attempt to scan.

How to Limit Login Attempts

While the above solution of changing your admin login URL can help decrease the majority of the bad login attempts, putting a limit in place can also be very effective. The free [Cerber Limit Login Attempts](#) plugin is a great way to easily setup lockout durations, login attempts, and IP whitelists and blacklists.



If you are looking for a more simple WordPress security solution, another great alternative is the free [Login Lockdown](#) plugin.

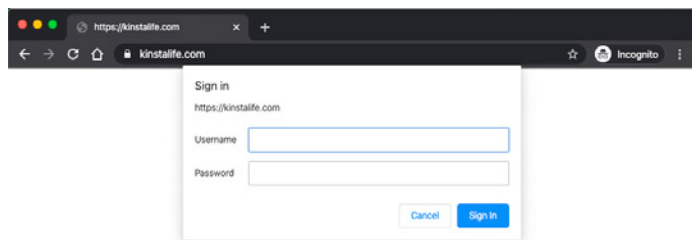


Login LockDown records the IP address and timestamp of every failed login attempt. If more than a certain number of attempts are detected within a short period of time from the same IP range, then the login function is disabled for all requests from that range. And it is completely compatible with the WPS Hide login plugin we mentioned above.

If you move your clients' site over to Kinsta, you don't need to install any additional plugin for our platform limits and blocks malicious attempts automatically.

How to Add Basic HTTP Authentication (htpasswd protection)

Another way to lock down your admin is to add HTTP authentication. This requires a username and password before being able to even access the WordPress login page.

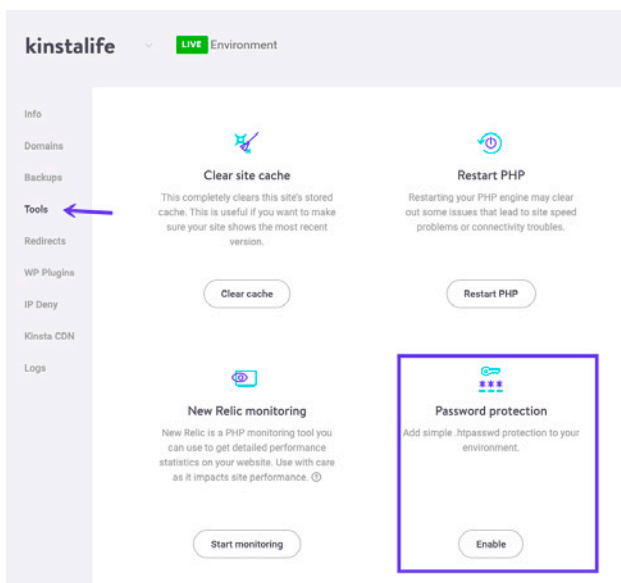


Check out this feature
with the MyKinsta demo.



Important: This generally shouldn't be used on eCommerce sites or membership sites. But it can be a very effective way to prevent bots from hitting your site.

If you host your clients' sites at Kinsta, you can use our easy [password protection \(htpasswd\) tool](#) in the MyKinsta dashboard (see it in action on the [free MyKinsta demo account](#)). You can find it under the "Tools" section on your site. Simply click "Enable", choose a username and password, and you're good to go!



Check out this feature
with the MyKinsta demo.



After it's enabled each WordPress site will then require authentication to access it. You can change the credentials at any time or disable it when you no longer need it.

Take Advantage of Two-Factor Authentication (2FA)

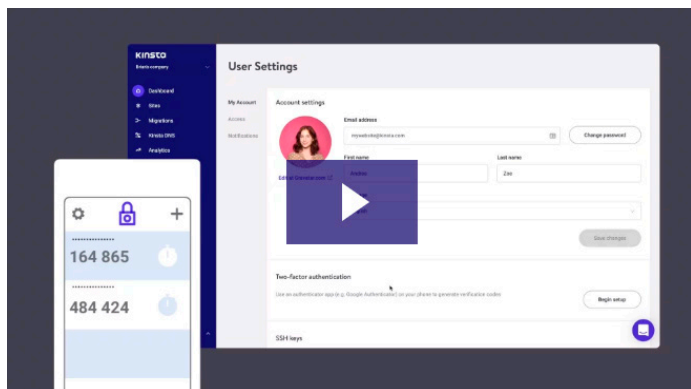
Two-factor authentication involves a two-step process in which you need not only your password to log in but a second method to log in. In most cases, this is 100% effective in preventing brute force attacks to your clients' WordPress sites.

There are two parts when it comes to two-factor authentication for client sites, though.

The first is your account and/or dashboard that you have with your web hosting provider. If someone gets access to this they could change all your clients' passwords, delete their websites, change DNS records, and all sorts of horrible things. We here at Kinsta use [Authenticator-based 2FA](#) for your MyKinsta dashboard because:

- Authenticator-based 2FA is more secure than SMS-based 2FA because it is not tied to your mobile phone number and doesn't rely on legacy SMS technology. This makes Authenticator-based 2FA resistant to SIM swapping techniques.
- Authenticator-based 2FA can be used with password manager apps like 1Password for added convenience. By adding your 2FA details to a password manager, you won't have to rely on an external device to log in to MyKinsta.

Here's how easy it is to enable it:



The second part of two-factor authentication pertains to your clients' actual WordPress installations. For these there are a few plugins you might want to test and recommend:

- [Duo Two-Factor Authentication](#)
- [Google Authenticator](#)
- [Two Factor Authentication](#)

After installing and configuring one of the above plugins on a client site, they will typically have an additional field on their WordPress login page to enter their security code. Or, with the Duo plugin, they'd first log in with their credentials and are then required to choose an authentication method, such as Duo Push, call, or passcode.

Use HTTPS for Encrypted Connections – SSL Certificate

One of the most overlooked ways to harden WordPress security is to [install an SSL certificate](#) and run sites over HTTPS. HTTPS (Hypertext Transfer Protocol Secure) is a mechanism that allows any browser or web application to securely connect with a website. A big misconception is that if your clients' sites aren't accepting credit cards they don't need SSL.

Well, let us explain a few reasons why HTTPS is important beyond just eCommerce. Many hosts, including Kinsta, offer free SSL certificates with [Let's Encrypt](#).

6 Key Reasons Why HTTPS is important beyond just eCommerce

1. Added Security

How important is your clients' login information? Well, you should know that every time a user logs in, that information is being passed to the server in plain text. HTTPS is absolutely vital in maintaining a secure connection between a website and a browser. This way you can better prevent hackers and/or a middle man from gaining access to your client's sites.

2. SEO

Google has officially said that HTTPS is a ranking factor. As most of your clients would probably take any possible advantage of SEO and SERPs to beat their competitors, this is a no-brainer.

3. Trust and Credibility

According to a survey from GlobalSign, 28.9% of visitors look for the green address bar in their browser. And 77% of them are worried about their data being intercepted or misused online. By seeing that green padlock, customers will instantly have more peace of mind knowing that their data is more secure.

4. Referral Data

A lot of people don't realize that HTTPS to HTTP referral data is blocked in Google Analytics. So what happens to the data? Well, most of it is just lumped together with the "direct traffic" section. If someone is going from HTTP to HTTPS the referrer is still passed.

5. Chrome Warnings

As of [July 24th, 2018](#), versions of Chrome 68 and higher started marking all non-HTTPS sites as "Not Secure." and, starting in 2020, the popular browser [started deprecating support for legacy TLS versions](#). Google is making it a lot more clear to visitors that a WordPress website might not be running on a secured connection. This is why HTTPS is more important than ever!

6. Performance

Because of a protocol called [HTTP/2](#), a lot of times, those running properly optimized sites over HTTPS can even see speed improvements. HTTP/2 requires HTTPS because of browser support. The improvement in performance is due to a variety of reasons such as HTTP/2 being able to support better multiplexing, parallelism, HPACK compression with Huffman encoding, the ALPN extension, and server push.

And with [TLS 1.3](#), HTTPS connections are even faster. Kinsta supports TLS 1.3 on all of our servers and our Kinsta CDN.

Check out our in-depth [WordPress HTTPS migration guide](#) to get you up and going and learn more in our [TLS vs SSL comparison](#).

Disable XML-RPC

In the past years, XML-RPC has become an [increasingly large](#) target for brute force attacks. There are a few WordPress plugins like Jetpack that rely on XML-RPC, but a majority of people out there won't need this and it can be beneficial to simply disable access to it.

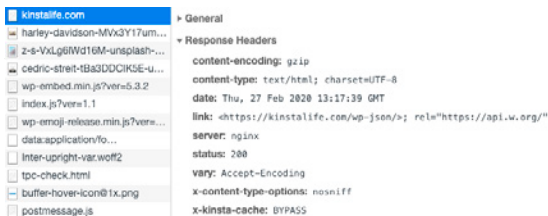
If you are a customer here at Kinsta, you don't have to worry about this as we have implemented active and passive measures to stop attacks and malicious intent in its tracks. Specifically, when an attack through [XML-RPC is detected](#) a little snippet of code is added into the Nginx config file to stop them producing a 403 error.

Add Latest HTTP Security Headers

Another step you can take to harden your client WordPress security is to take advantage of HTTP security headers. These are usually configured at the webserver level and tell the browser how to behave when handling your client sites' content. There are a lot of different HTTP security headers, but below are typically the most important ones.

- [Content-Security Policy](#)
- X-XSS-Protection

- [Strict-Transport-Security](#)
- [X-Frame-Options](#)
- [Public-Key-Pins](#)
- [X-Content-Type](#)



Here's an example on [kinstalife.com](#) (a demo site). You can see we are utilizing the `x-content-type-options` header.

When it comes to client sites, like in the example shown, `x-content-type-options` is always added by default, while `x-frame-options` and `strict-transport-security` are set only if required.

If you need to scan your clients' sites, you could do that with the free [securityheaders.io](#) tool by Scott Helme.

It is also important to remember that when you implement HTTP security headers how it might affect your [WordPress subdomains](#). For example, if you add the Content Security Policy header and restrict access by domains, then you need to add your own subdomains as well. If you aren't sure how to implement them you can always ask your host if they can help.

Use WordPress Security Plugins

There are a lot of great developers and companies out there which provide great solutions to help better protect your WordPress site.

Notable ones are:

- Sucuri Security
- iThemes Security
- Wordfence Security
- WP Security Audit Log
- WP fail2ban
- All In One WP Security & Firewall
- SecuPress
- BulletProof Security
- VaultPress
- Google Authenticator – Two Factor Authentication
- Security Ninja
- Defender
- Astra Web Security
- Shield Security
- Hide my WP
- WebARX

Kinsta has hardware firewalls, active and passive security, by-the-minute uptime checks and scores of other advanced features to prevent attackers from gaining access to your data. If, despite our best efforts, your site is compromised we'll fix it for free.



A very important feature that many security plugins include is a checksum utility. What this means is that they inspect each of your client’s WordPress installations and look for modifications on the core files as provided by WordPress.org (via the API). Any changes or modifications to these files could indicate a hack.

You can also use WP-CLI to [run your own checksum](#). Check out these additional [WordPress security plugins](#) that can help lock out the bad guys.

Harden Database Security

There are a couple of ways to improve the security of your WordPress database. The first is to use a clever database name. By changing your database name to some more obscure it helps protect their site by making it more difficult for hackers to identify and access your database details.

Below you should enter your database connection details. If you're not sure about these, contact your host.

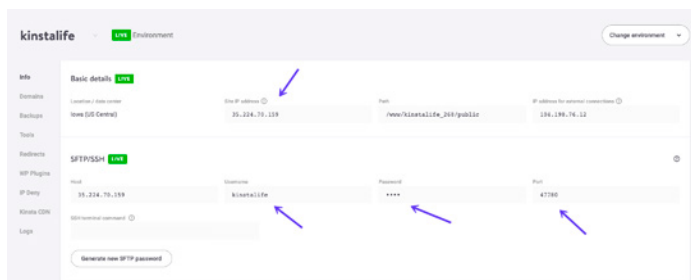
| | | |
|---------------|----------------------------------------|----------------------------------------------------------------------------------------|
| Database Name | <input type="text" value="wordpress"/> | The name of the database you want to use with WordPress. |
| Username | <input type="text" value="username"/> | Your database username. |
| Password | <input type="text" value="password"/> | Your database password. |
| Database Host | <input type="text" value="localhost"/> | You should be able to get this info from your web host, if localhost doesn't work. |
| Table Prefix | <input type="text" value="wp_"/> | If you want to run multiple WordPress installations in a single database, change this. |

A second recommendation is to use a different database table prefix. When you install WordPress, it asks for a table prefix. By default WordPress uses `wp_`. Changing this to something like `39xw_` can be much more secure.

If you're a Kinsta client and host all your clients' sites with us, this isn't needed. We've got site and database locked down for you!

Always Use Secure Connections

We can't stress enough how important it is to use secure connections! Ensure that your WordPress host is taking precautions such as offering SFTP or SSH. SFTP or Secure File Transfer Protocol (also known as SSH file transfer protocol), is a network protocol used for file transfers. It is a more secure method vs standard FTP.



Check out this feature
with the MyKinsta demo.



We only [support SFTP connections](#) at Kinsta to ensure your data remains safe and encrypted. Most WordPress hosts also typically use port 22 for SFTP. We take this a step further here at Kinsta and every site has a randomized port that can be found in [your MyKinsta dashboard](#).











Check File and Server Permissions

File permissions on both your clients' installations and web servers are crucial to beefing up the security of these environments. If permissions are too loose, someone could easily gain access to their site and wreak havoc. On the other hand, if your permissions are too strict this could break functionality on their site. So it is important to have the correct permissions set across the board.

You can use a free plugin like [iThemes Security](#) to scan the permissions on your clients' WordPress sites.

File Permissions

Reload File Permissions Details

| Relative Path | Suggestion | Value | Result | Status |
|--------------------|------------|-------|---------|-----------------------------------------------------------------------------------|
| / | 755 | 755 | OK |  |
| wp-includes | 755 | 755 | OK |  |
| wp-admin | 755 | 755 | OK |  |
| wp-admin/js | 755 | 755 | OK |  |
| wp-content | 755 | 755 | OK |  |
| wp-content/themes | 755 | 755 | OK |  |
| wp-content/plugins | 755 | 755 | OK |  |
| wp-content/uploads | 755 | 755 | OK |  |
| wp-config.php | 444 | 644 | WARNING |  |
| nginx.conf | 444 | 644 | WARNING |  |
| Relative Path | Suggestion | Value | Result | Status |

Here are some typical recommendations for permissions when it comes to file and folder permissions in WordPress:

- All files should be 644 or 640. Exception: wp-config.php should be 440 or 400 to prevent other users on the server from reading it.
- All directories should be 755 or 750.
- No directories should ever be given 777, even upload directories.

See the WordPress Codex article on [changing file permissions](#) for a more in-depth explanation.

DDoS Protection

DDoS is a type of DOS attack where multiple systems are used to target a single system causing a Denial of Service (DoS) attack. DDoS attacks are nothing new – according to [Britannica](#) the first documented case dates back to early 2000. Unlike someone hacking your site, these types of attacks don't normally harm your site but rather will simply take your site down for a few hours or days.

What can you do to protect yourself? One of the best recommendations is to use a reputable 3rd party security service like Cloudflare or Sucuri.

Their advanced DDoS protection can be used to mitigate DDoS attacks of all forms and sizes including those that target the UDP and ICMP protocols, as well as SYN/ACK, DNS amplification and Layer 7 attacks. Other benefits include putting you behind a proxy which helps to hide your origin IP address, although it is not bulletproof.

Don't overlook the provider your web host uses because that's also pretty important.

Hardware firewalls, such as the Google Cloud Platform Firewall we use at Kinsta, are in place and have very tight software-based restrictions to protect your clients' sites and also have software in place to [detect DDoS attacks](#) as they happen.

This means you and your clients get the benefit of a security model that has been built upon over the course of 15 years, and currently secures products and services like Gmail, Search, etc. Google currently employs more than 500 full-time security professionals.

On top of Google Cloud Platform, we also use Linux containers (LXC and LXN) to orchestrate them, which enables us to completely isolate not just each account, but each separate WordPress site.

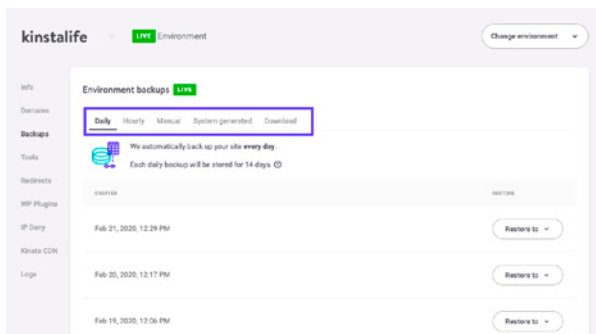
Things go South nonetheless? Kinsta provides free hack repair and [malware removal](#). If one of your clients' sites is infected, our support team will do all that it takes to clean it up.

Get more details about how seriously we take security at Kinsta!



Always Take Backups

No matter how secure your site is, it will never be 100% safe. That's why you want backups in case the worst happens. Backups are the one thing everyone knows they need but don't always take. Most of the recommendations here outlined are security measures you can take to better protect your clients' sites and your business.



Check out this feature
with the MyKinsta demo.



Most managed WordPress hosting providers now provide backups. Kinsta has five different types of backups:

- **Daily:** Kinsta creates [automated backups](#) of all your clients' sites every 24 hours so that you can rest easy at night.
- **Hourly:** If you need a more frequent backup schedule, you could activate 6-hour or hourly automated backups for any target site that requires it (this comes on top of your monthly plan).
- **Manual:** if automated backups aren't enough, you can create manual backups for each site you're managing and have this additional copy available for 14 days or more, based on your current plan.
- **System generated:** before critical tasks such as using the search-replace tool in MyKinsta, pushing a staging environment live, and restoring a backup to your live environment, Kinsta will trigger system-generated backups.
- **Downloadable archive:** if all this isn't enough, once per week, you could download a zip file of each client site containing website files and an SQL file containing the contents of the site database.

Backup options don't come alone as Kinsta allows you to easily restore any site with a single click. That's convenient, isn't it?

**Test for free how easy
is creating backups with MyKinsta!**



If your host doesn't have backups there are some popular WordPress plugins that you can use to automate the process.

WordPress Backup Plugins

WordPress backup plugins allow you to grab your backups via FTP or integrate with an external storage source such as Amazon S3, Google Cloud Storage, Google Drive, or Dropbox. We highly recommend going with an incremental solution so it uses fewer resources:

- Duplicator
- WP Time Capsule
- BackupBuddy
- UpdraftPlus
- BackUpWordPress
- BackWPup
- WP BackItUp

Kinsta doesn't allow non-incremental backup plugins due to performance issues: we handle all this for you at a server-level so it doesn't slow down your clients' sites.

Summary

Security is a layers game. The more you're successful in stacking new security layers on top of one another, the more secure your clients' sites will become. It all starts with using clever passwords, keeping core and plugins up to date, and following other security best practices we've covered here.

But that's not all you should do to lower your chances of having to deal with hacked client sites. By choosing a managed WordPress host like Kinsta, most of the security measures are taken care of for you, allowing you to build a solid, secure, and scalable foundation to securing the future of your clients' sites. And that of your business.

Want to try how easy it is to manage client sites on Kinsta?

Check out
[demo.mykinsta.com!](https://demo.mykinsta.com/)





KINSTA