\

The #UpdraftPlus Guide to WordPress Security

"I run a service that deals directly with client sites that have been compromised. Poor password management and poor plugin and theme security coding practices most often being the cause, but the main reason is that clients (either because of fear, or inattention fail to update their sites properly. The recovery fees we charge include deep scans, cleansing, full tested updates, and password hardening, among other services. If can obviously be a shocking experience for site owners, especially for business owners, when a site is hacked. There can be serious, even unrecoverable consequences for reputation and confidence."

- survey response

Introduction

In 2003, WordPress was just a single bit of code used by a handful of people for blogging. Now it's the largest self-hosted website building tool in the world.

And refreshingly, WordPress is available freely to anyone: it's Open Source, meaning it's built, run and owned by the community. Anyone can contribute by offering support, writing patches and plugins or creating themes.

Unfortunately, there are those who enter the WordPress community with criminal intent. Thousands of WordPress websites are hacked every day, and not just minor ones.

In fact, people are trying to break into your WordPress website basically all the time. This comes as a shock to some, because it's easy to be unaware of what's going on, until it's too late.

Hacker Motives

But why do hackers want to do this anyway? Motives vary; there are plenty of people who think that destroying things is fun.

However, the main motive is a predictable one: profit. There's money to be made. This at first seems surprising: after all, where's the money to be made in a little blog?

If a Website doesn't make money for its owner, how can it profit anyone else? Well it can, and here are the main 3 ways:

1. Computing Power, "free" and anonymous

It's not your website itself that the average attacker wants; they want the computer power of the webserver that it's running on. They want the free electricity. This can be used to perform complex computations such as those used to "mine" digital currencies like Bitcoin, or simply to hide the hacker's identity whilst he uses a server not linked to his name to perform other tasks.

2. Spam, spam, spam spam…

That computing power can also be used to churn out millions of spam emails, again, for free (to the attacker) and in a way that's hard to trace, since the emails will come from your server rather than the attacker's own computers. Since emails are quick and easy to send, often by the time it is spotted, the attacker has got his pay-off.

Spam equals money. Sadly, there are people who don't immediately delete them and instead reward the evil business model. Website owners and hosting companies have to pick up the tab when the addresses of their servers get black-listed as spam sources, and time has to be invested in cleaning up.

Another way is to insert links into web pages of sites selling things, like various pharmaceuticals. These links may not even be intended or visible for people to click on, but they are visible to search engines and help the destination websites move up the search rankings. Unscrupulous marketeers can find it much cheaper to buy space on a thousand hacked websites from shady operators than to build up genuine interest in their products.

3. Serving up Viruses

A hacked website can be modified to serve up viruses to its visitors, catching vulnerable visitors whose own computer security wasn't up to date. Viruses then allow the visitor's computer to be used for the same purposes – and some others. For example, some viruses will encrypt all your files, and decrypt them only upon payment of a ransom, i.e. "ransomware". Or they may inject new adverts into every web page you visit, making money for either the sellers of advertising space or the sellers of the advertised products. They may log clicks and keypresses on the computer and capture valuable passwords, e.g. for online banking.

Sadly, insecure websites are economically valuable. Weak passwords, un-updated plugins, etc., provide ways for the bad guys to use your computing resources to make money. The costs of breaking in are less than the revenues they can make, so hacking is a profitable activity.

The Cost to You

So even if your website is small and doesn't make you any money, it could still make hackers rich. And unfortunately, if they have their way, you lose- bigtime. You lose time, money and face.

If you've got an online business, your customers' and clients' personal information could be stolen. You could untold sums of money- and it happens even to vast multinationals when they let their guard down.

Even if the cost isn't financial, a cyberattack could knock your SEO ranking, making it harder for customers to find you. It will also give your reputation a nasty blow, as people lose confidence in you and your brand. Google is very vigilant when it comes to sites that have been attacked, and it doesn't discriminate: "*Safe Browsing shows people more than 5 million warnings per day for all sorts of malicious sites and unwanted software, and discovers more than 50,000 malware sites and more than 90,000 phishing sites every month.*"

And don't underestimate the emotional cost. This Sucuri blog reminds us of the "*hours you will spend arguing with hosting providers, developers, security profession-*

als …the fear that you missed something in the clean-up process…the new fear of being online at all, of using technology as a whole. All this is exasperated by one simple thought, "Why didn't I take precautions?"

To what extent would it affect you if your website was hacked today without any security measures?

Are You Safe?

Which brings us to the point: are you safe?

WordPress is constantly working to improve its security, and over the years, the number of vulnerabilities has decreased. However, in that period, the number of hacks has increased simply because the high number of users makes it an extremely attractive target. Whatever vulnerabilities there are, cybercriminals have a strong incentive to find and exploit them.

WordPress is actually pretty secure out of the box, but its Plugins, Themes and Custom Code with PHP code written by all manner of developer massively increases its exploitable vulnerabilities. Indeed, by far the majority of WordPress sites are weakness in WordPress are due to poor software, flaws in the interaction with WP or web server errors, rather than through a vulnerability in the Core platform.

There's no such thing as total security. However, there are simple things you can do to greatly reduce your chance of becoming a victim. Most cyber-attacks are automated, run by bots that constantly probe for specific exploits.

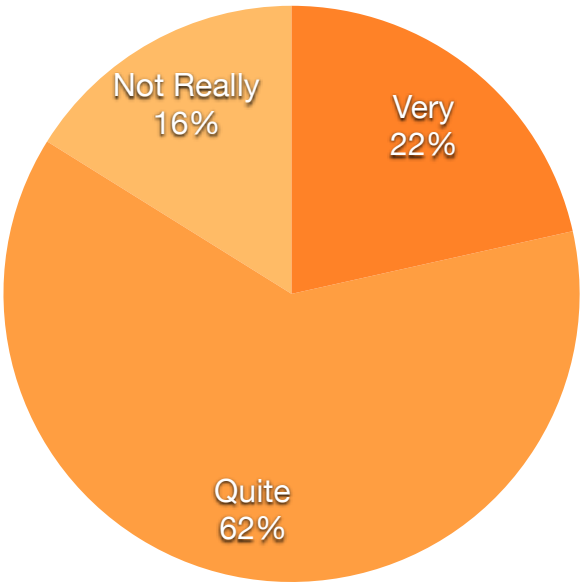
Like Health and Safety, practising Good Cyber Security isn't something people get excited about, but it is incredibly important.

Hackers can always pick off the weakest: WordPress users who don't keep up-to-date with installs, who are self-hosted and slack, and who fail to take basic security precautions. With millions of users, there will always be tens of thousands of potential victims out there.

If you're not aware of the risks and you don't take measures to protect your website, you're setting yourself up for a fall.

But what should you do? We've put together a little guide to keeping your WordPress site safe.

How resilient would you consider your WordPress site to be against being hacked now?



Guide to keeping your WordPress website safe

1. Use the latest version of WordPress and WordPress Themes and Plugins

Making sure that you always install the latest, updated versions for WordPress Core plus Themes and Plugins as they're released is by far the easiest and most important way to shore up your security and functionality whist avoiding bugs.

Say they keep up to date

Why?

As soon as new software is released, hackers get to work sussing out security loop-holes in operating systems by watching the release notes to seek out vulnerabilities. As soon as they find one, they start to exploit it. New versions are then released to patch up these vulnerabilities and strengthen against attacks.

Of course, because the new updates often mention the security loopholes they've closed, the hacker has an easy time exploiting it if he sees you're using that older version. You're making their job easy.

WordPress founder Matt Mullenweg tries to press home why upgrading is so important: "WordPress is a community of hundreds of people that read the code every day, audit it, update it, and care enough about keeping your blog safe that we do things like release updates weeks apart from each other even though it makes us look bad, because updating is going to keep your blog safe from the bad guys. …as long as WordPress is around we'll do everything in our power to make sure the software is safe."

He Continues: "A stitch in time saves nine. Upgrading is a known quantity of work, and one that the WordPress community has tried its darndest to make as easy as possible with one-click upgrades. Fixing a hacked blog, on the other hand, is quite hard. Upgrading is taking your vitamins; fixing a hack is open heart surgery."

Some WordPress updates don't include security patches- typically, the major ones (i.e. the ones with a single number after the decimal, such as 4.3). Where they don't, there isn't such a pressing hurry to update. However, the latest versions are generally the safest, and it's good practice to update as soon as possible.

How to Stay Up-to-Date

- Identify which version of WordPress you are using.
- If you're not using the latest stable release of WordPress (Version 4.3.1), download it now. It's extremely quick and easy.
- Some Web Hosts, e.g. WP Engine, will keep WordPress updated for you automatically.
- To keep track of your WordPress Themes and Plugins and to keep them updated at all times, use a tool like Jetpack.
- In the case of a security breach, always restore your site from the backup, so that backdoor attackers can never open old exploits.

Even in the most recent releases of WP, there are known security issues, so check your version against the known vulnerabilities.

2. Only Install Good WordPress Themes and Plugins

Be extremely cautious with the WordPress Themes and Plugins you install, as many of these are insecure, hacked, bloated or out-of-date.

Why?

There are over 40,000 free WordPress Plugins available. By extending the WP CMS Core functionality, these Plugins can make WordPress do virtually anything. They represent the 'beating heart of WordPress' and have been central to its exponential growth.

However, not all Plugins are secure. This is to be expected, as anyone can contribute. As well as being a massive plus, WordPress' Open Source nature is also its Achilles heel. Because there are so many out there, there will always be some that are bad, hacked, poorly maintained and rarely updated. According to a survey of 170,000 hacked websites in 2012 in WpWhiteSecurity's blog, a striking 51% were hacked via a security issue in a WordPress Plugin or theme.

Although the WordPress core is extremely secure, Plugins can cause havoc. A WooThemes article on the subject puts it like this: “When we install a plugin, anything can happen. Your website’s load speed can be seriously affected. It can even crash entirely. In fact, some unscrupulous developers create bad plugins (or hack into otherwise trustworthy plugins) with no other aim than to cause others pain. These are the possibilities we face every time we click on Activate.”

Tips on how to avoid dodgy Plugins and Themes…

- Purchase only from developers that have a solid and well-established reputation.
- Use commercial Plugins, as security vulnerabilities are dealt with quickly. They cost more than free alternatives, of course, but the vendors have more to lose.
- If it’s free, ensure that it has a large number of downloads, high ratings and that it brings out regular updates.
- Explore its history; check that old versions have the same author as new ones.
- Minimise the number of installed Plugins/Themes you use: you’ll be surprised how little functionality is affected, and you may be able to replace some with simple code snippets.
- Use a Plugin to track everything that runs on your sites, particularly if you’re in charge of multiple sites. This enables you to notice problems and source their trace as soon as they occur.

3. Guard your logins

The WordPress Login Page is a prime target for brute force attacks. Your login page is vulnerable, and using weak passwords and usernames is like leaving your front door unlocked.

Why?
Sometimes hackers don’t exploit software vulnerabilities; instead, they target “the weakest link in any website's security: You.”

Brute force attacks try common passwords and usernames over and over again until they work. This may seem rather primitive, but by using a botnet, hackers can get through hundreds of combinations per minute. When you don't bother changing the default 'Admin' username, or you chose a password like "Password123", "123456" and "qwerty", you make such attacks pay off.

Once hackers succeed in this way, they can do virtually anything, as a WordPress user describes: "if someone else is able to guess or retrieve your password, they bypass almost every security measure we have because WordPress.com will see this person as you. They could then make any changes they wish to your WordPress.com blog or account including the deletion of your content."

What's more, if you use the same username or password for other accounts such as your email, online banking or social media account, the hacker can easily leverage their access, leaving you the victim of identity theft, account spanning or worse.

How to keep your Logins Secure
If you haven't changed your WP Username, do so now! Here's how.

Don't choose a random string of letters, numbers and figures which are hard to remember but easy for the latest computers to guess. Instead, either use…

1. A Password Manager: this is an App that generates and stores very strong passwords, which you can access through a passphrase.

2. A Passphrase: better than a password, this is a random collection of words, such as happy long elephant go.

If you do use a password, make sure it mixes upper and lowercase letters with punctuation and special characters. It should be meaningless, and at least 10 characters long.

WP Password Policy Manager, Force Strong Passwords or Enforce Strong Password are useful at helping you to come up with strong passwords (WordPress 4.3 and onwards also helps in this area).

Make sure you set a limit on the number of attempted Logins from a single IP address. WordPress shows you how here.

Always remember to use unique usernames and passwords for each different online account.

4. Use a Reputable Web Service Provider

If you pick the wrong web host, your site stands is much more vulnerable to getting hacked.

Why?
Most people are surprised that a third-party host can play such a critical part in keeping your website safe.

Poor web host providers are those who run their systems on software (i.e. anything that keeps your site live like PHP, MySQL, SSL certificates, etc.) that's out-of-date or poorly maintained. If it's not current or maintained, any past vulnerabilities in this software are open for exploitation.

Sometimes, web hosts providers have a range of other bad security practices such as storing users' passwords in a non-hashed format and lack of access controls meaning other users can access your website files.

Although shared hosting is more affordable for new businesses, it does carry higher risks:

- DOS attacks on one IP server can affect all
- Shared IP addresses mean problems with neighbouring IP addresses affect your own
- Problematic software loaded on a shared server can compromise the whole thing.

How to pick a decent Web Server Host

Don’t just go for the cheapest option! You’ll probably get what you pay for. Instead, ensure you use a well-established company with a strong reputation and a good track-record for security.

If you are going for shared Web Hosting…

- Choose a Host with strong security features and account isolation to protect you against vulnerable websites on the same server.
- Check your Hosts screen accounts carefully, and avoid those that offer open access, cost-free or advertisement-sponsored accounts.
- Ensure your Host uses a reliable clustered firewall, a 24-hour monitoring system and a means of backing up sites on a daily basis.

Use a CDN system such as CloudFlare to protect against DDoS attacks.

Managed WordPress hosts are more secure (and faster); if you can afford to use these instead, you should. Note, although the cost is high, so is the cost of losing everything through hacking.

5. Use 2-Factor Authentication:

Two-factor authentication is one of the strongest ways to keep your Login safe.

Use 2-Factor Authentication

Why?
With Logins the most vulnerable port into your account, and two-factor authentication makes brute force attacks much more difficult to pull off.

So what is Two-factor authentication? Google’s Matt Cutts describes it as “a simple feature that asks for more than just your password. It requires both "something you know" (like a password) and "something you have" (like your phone). After you enter your password, you'll get a second code sent to your phone, and only after you enter it will you get into your account. …It's a lot more secure than

a password (which is very hackable), and keeps unwanted snoopers out of your online accounts."

How to add another layer of WordPress Login Security

WordPress.com now offers two-step authentication via mobile device. Every time you log in with your password, WordPress will send a new code to your device, which you have to type in before you can Log In to your account. It adds a few seconds more but greatly increases security.

Have SSL Certificates

6. Get an SSL certificate
7. SSL (Secure Sockets Layer) is a technology for verification (so that you know who you're really talking to) and for encryption (so that your communication cannot be snooped upon by anyone else along the way).

Why?

SSL is a way of securing network communication links. Without it, third parties can potentially listen in to communications between your website and the end user.

Eavesdropping can lead to sensitive private data being stolen, and can pose a real risk to individual users. If a User accesses your website from a public WiFi connection, others in the same location can potentially see what is being typed on non-SSL-protected forms fairly easily. Financial transactions, usernames and passwords, and banking details are at risk without SSL, and the consequences can be serious.

Having an SSL certificate prevents this kind of eavesdropping; the padlock icon at the top of the webpage address not only assures Users that their data is safe, it also validates your website's identity, assuring them that they are not visiting an imposter site.

SSL can also require private IP addresses, if you need to be compatible with older browsers (such as Internet Explorer on Windows XP, or Android version 2.2) which may incur an extra cost if you do not already have a private server.

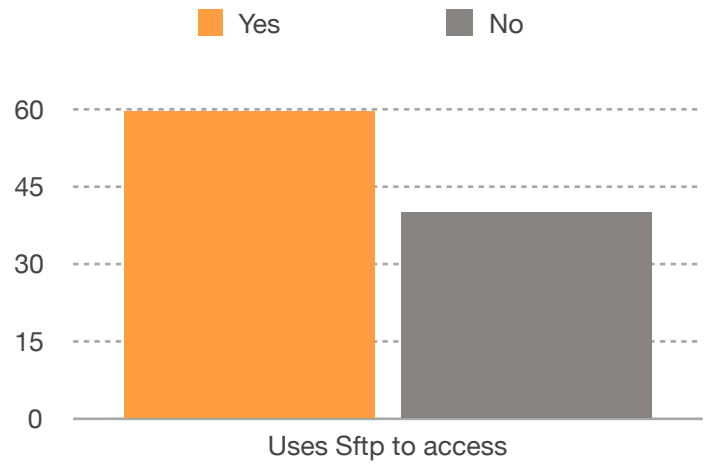
How to get an SSL Certificate

You should be able to purchase and apply an SSL Certificate from your Web Host provider.

There's a bit of bureaucracy involved in setting things up- as this article explains, you will need (the requirements vary depending on your setup and specific SSL needs) a unique IP address for each certificate you want, a CSR, a correct WHOIS record and business validation documents.

Once established, renewal is easy for a small fee.

8. Use SFTP Instead of FTP to Access the Server



File Transfer Protocol (FTP) is a well-established way of using the internet to transfer data between computers. As this SRT article describes how the conversation between the FTP client and the server is performed in plain text: "all communication between the two parties is sent unprotected, verbatim, over the internet. This makes FTP very unsecure; it would not be terribly difficult for a third party, such as a Man-in-the-Middle Attacker (MITMA), to steal users' credentials."

When you open up a conversation view FTP, the whole transmission between host and user can be snooped on by anyone who can see the network packets; it means that unauthorized users also have the opportunity to compromise the system.

Using Secure File Transfer Protocol (SFTP) instead means that data is communicated over a single secure, efficient connection through the firewall. SFTP encrypts the entire Login session, making it much more difficult for an outsider to view and collect passwords. As an alternative, some FTP servers allow you to configure your FTP program to use encryption, instead of plain vanilla FTP – but this requires you to make sure you're doing it correctly.

How?
Here's a guide to transferring data using Sftp.

9. Use Security Plugins

It's worth installing Security plugins to further tighten your site's security and reduce the chance of being hacked.

Why?
This ManageWP Blog explains their value: "Primarily, security plugins provide an added layer of protection against brute force attacks and malware. They give you a set of tools, that when properly configured, help to put some of the main security tasks you'd have to complete on a regular basis on autopilot. The best plugins also help you to recover more quickly from a hack, should you fall victim to one."

Think of Security Plugins as your WordPress Site's bodyguard: they can detect Malware and vulnerabilities, suspicious activity and bots. They also offer other features to help you stay on top of other security measures, such as tools to update WordPress automatically, to change your "Admin" username and to test password strength (for example).

How to get a Security Plugins

There are a number of good WordPress Security Plugins out there. The most popular and well-known include

- iThemes Security
- All in One WP Security & Firewall
- Sucuri Security
- Wordfence Security
- BruteProtect
- Acunetix WP Security
- Bulletproof Security

These each have different features, so you may want to explore what each offers before you make a decision.

10. Always Back Up!

Making regular backups of your website plus all files and databases is vital.

Back up to a remote storage location

Why?

You make take every single security precaution going, but the reality is, you're never 100% safe.

You need to keep regular backups, so that if something terrible did happen, you could restore everything in a matter of minutes to a safe location away from your live site.

How to back up like a Pro:

Backup plugins makes keeping your WordPress site easy. When choosing a provider, ensure that it's secure, trusted, well-established, easy-to-use and comprehensive. You might want to check its features and capabilities, too.

Obviously, we recommend UpdraftPlus, which is extremely popular, reliable and trusted! Don't just take our word for it, check out its WordPress Reviews.

Advice when using backups:

- Set up an automatic backup schedule so that you won’t ever forget to make regular backups.
- Remember to back up not only your website but also its databases Themes, Plugins and Uploads. You can also save your WP Core and Content, plus any other files and databases on your server.
- Make sure you send your backups to a remote location – don't just keep the backups on the same webserver as the website is on, as then an event which causes the loss of your website could lose your backups too.
- Encrypt database backups for security

10% of respondents in our latest WordPress Survey said they think a hacking incident would barely affect their website. Presumably, these respondents are 100% confident in their UpdraftPlus backups.