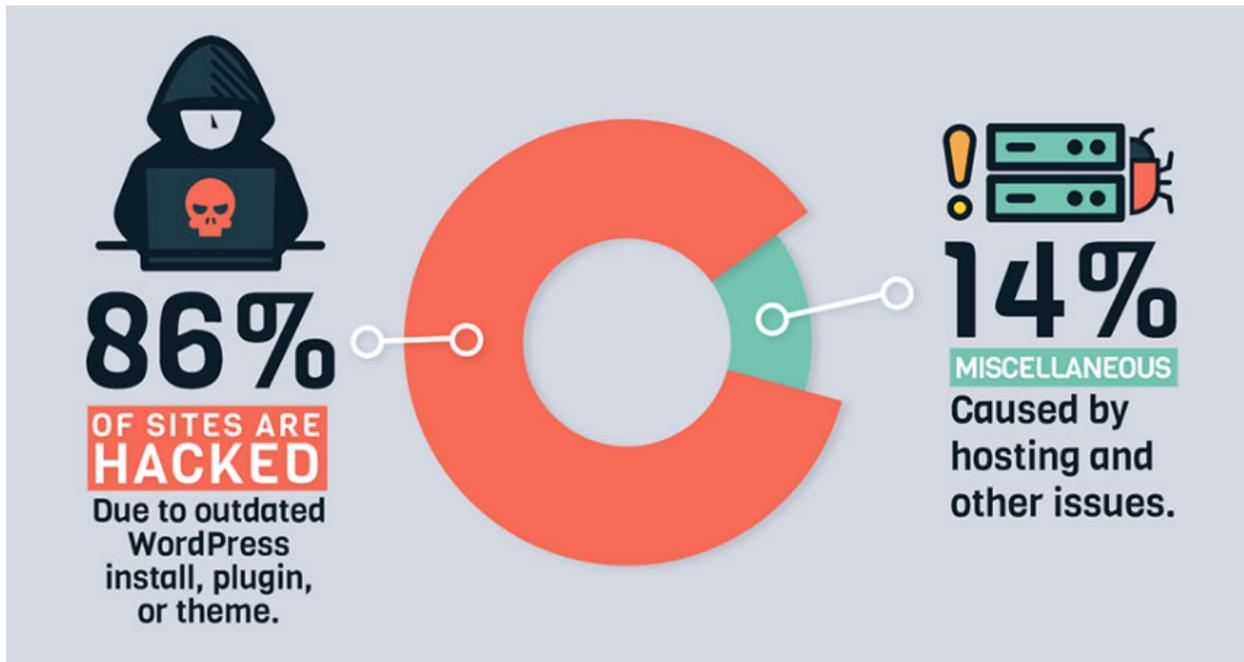


WordPress Security, Maintenance and Oversight (a.k.a. Building a website is only half the battle)



Just like your computer or your phone, to keep running smoothly, your website needs to be backed up and updated regularly – once a month is a bare minimum.

Updating *all* the software that runs your website **increases security, fixes bugs, and adds features and functionality.**

The more time that passes between updates, the more likelihood that updating will cause a conflict and break your site to some degree.

More than 1/3 of *all websites worldwide* are built on the WordPress platform. This means that WordPress websites are the most obvious targets for hackers, and every site is at risk because, as a general rule, the hackers don't care about your site at all, they just want to access your hosting server. You may not even know that your site has been hacked until Google blacklists it or your host takes it down.

The good news is that the WordPress community is vast, vigilant and helps each other. Because of this, security vulnerabilities are most often found and fixed before they are exploited. How are they fixed? By sharing information and constantly releasing new versions of the core, themes, and plugins.

CJBuilt offers various security, maintenance and oversight plans for WordPress websites

For most websites that have no e-commerce components (on-site sales, taking of credit cards, etc.), my recommendation is a bi-weekly plan.

Specifically, what this means is that twice a month, on or around the 1st and the 15th, I will:

- Visit your site and make sure everything is functioning properly.
- Log in to the site and check the security report from the last two weeks which includes blocked IPs, log-in attempts, file changes, attempts to inject malicious code, etc. and immediately address any concerns.
- Create a backup of the entire website.
- Run all available software updates.
- Re-visit the front end for a comprehensive functionality check.
- Resolve any issues that arise (up to 30 minutes at no additional charge).
- Create another full backup and send a copy to my secure cloud storage.

Additionally:

- Your website will be automatically scanned every day for malicious code, backdoors, shells that hackers have installed, known malicious URLs and known patterns of infections. All your posts, pages and comments will be examined for malicious code, injected links, and URLs that do not belong.
- Two months of full backups will be stored on your server in to facilitate a roll-back to a pre-hacked state even if the hack is not detected immediately.
- A copy of the most recent full backup is stored off-site in a secure cloud storage platform to protect against catastrophic server failure or gross human error.
- Websites that include an active blog or other frequently updated content will have the database automatically backed up every day.
- I will receive an email alert if a scheduled back up fails for any reason.
- If your website goes down or if malware is detected I will receive an email alert immediately and will address the situation as soon as I am able.
- I subscribe to several security blogs, and if I receive information about the discovery of a security vulnerability with the potential to impact your website, I will close the vulnerability as soon as I am able, regardless of where we are in the two-week cycle.
- I will give you notice when I will be unavailable for a substantial period, i.e. on vacation. If I go off the grid entirely, I will provide you with a contact person who is equipped to address any emergencies which may arise with your website.
- Small changes to the *existing content* of your website (up to 30 minutes per month) are included.



The Most Important Part:

I run through this entire process at a time when I am prepared to address with any issues that arise. If you choose to do your own maintenance, or choose to just let it go without updates, eventually something is going to break and odds are that it will be when I am on vacation and unavailable. This is not meant as a scare tactic, but just fair notice that I will *not* drop everything and address your broken website in the absence of an ongoing maintenance contract.

And a disclaimer:

A maintenance contract does *not* guarantee that your site will never go down or be hacked, but it dramatically decreases the chances and makes the recovery process much faster and less time consuming.

Non-CJBuilt Websites

For websites that I did not build I need to charge an additional initial set up fee that covers familiarization, evaluation, and bringing the software and security structure up to my standards, which includes installing premium plugins that I license for this purpose.

Investment

To generate a personalized quote, I need to perform an initial assessment of your website for which I need to have administration level access to your WordPress dashboard.

The monthly subscription cost will be auto-paid in advance via PayPal. A PayPal account is not required. The subscription may be cancelled at any time but no refunds will be given.

The set-up fee, if any, will be paid in advance of the set-up taking place.

Access

To perform the maintenance described herein I need to have both admin level access to your WordPress dashboard and access to your hosting account.

Contact me for a quote today.

