Website Security Checklist

* Run an anti-virus scan on your local computer, cleaning up any infected files.
* Clean-up your account. You can check out our article which describes how to clean up your account from malicious code:
* https://www.siteground.com/kb/how\_to\_clean\_my\_files\_from\_malicious\_code/
* Change your cPanel password, as well as the passwords for the installed applications on your account.
* Update any applications installed on your account and their components to the latest available version.
* Two step authentication
* Enable a Website Firewall – WAF: There are a growing number of software vulnerabilities, being exploited by attackers. Trying to keep up with them can be very challenging to you as a website owner. This is where a Firewall comes into play. It will stop attacks before they can reach your website. Note, that it will only start protecting your site after you activate it by changing your site's DNS settings.
* Update your website! If you are using WordPress, Joomla (or any other CMS), please update it to the latest version. Why? Because out-of-date software is the leading cause of infections. This also includes your plugins, themes, and any other extension type.
* Change your passwords: Change the passwords related to your website: FTP, SFTP, cPanel, Plesk, WP-admin, etc. They could have been compromised and we do not want you to be reinfected because the attackers can still come back in through them.
* \*Password Tip: Start using a password manager like: Peguta or LastPass. They're online and free.
* Change your database password. If you are using a CMS (WordPress, Joomla, etc…) change your database password. Please be sure to update your configuration file – Joomla: configuration.php and WordPress: wp-config.php. This is not an automated process so you will need to know how to open those files and edit manually. If you’re not familiar with handling changes in your database and configuration files, contact your host. \*If you don’t know how to change your passwords (specified above), contact your hosting company for details. You can also Google for “YOUR HOSTING COMPANY – FTP password” for instructions how to do so.
* Run a virus scan on your personal desktop/laptop. In a lot of cases we see that websites are compromised due to a desktop malware that steal credentials. It's why we always ask you take a minute to run an antivirus product. There are multiple options that you can choose, including BitDefender, Kaspersky, Norton and Sophos. We also recommend looking at additional tools to protect your desktop, like Malwarebytes (Windows and Mac) and CleanBrowsing(DNS-based).
* Backup your site: After the site is clean and secure, a very good practice is to do daily backups at a minimum. There are a number of backup solutions out there you can use. If you are a client of ours you can sign up for our Website Backup solution. It’s a simple configuration that works off FTP / SFTP and stores all your content, including the database, in the cloud.
* Security WordPress Plugin.
* Clean your Kitchen. Too often the issues we see plaguing our clients are caused by “soup kitchen” servers. Old installations of their content management systems, themes or plugins. Over time these old installs become forgotten but grow ripe with malware that’s ready to infest their entire server after each clean. Take a minute to separate those things that belong on a test, staging and production server.