http://prospermountain.com/whole-enchilada-security-pack/

So what's included in our **Security Packs**?

First, our goal is to keep everything as simple and unobtrusive to the website owner as possible. For the normal interaction with their website, very little will seem different. Most of the power of our packages lie "under the hood" protecting a site, but never getting in the way.

So here's what included:

- Before we start applying our Security Packs we do a little prep.
- Your whole site is backed up
- We scan your site for malware or blacklisting
- We scan your themes and plugins for compliance with best WordPress standards
- We bring your site up-to-date

(In some cases we may find issues that we are either unable or uncomfortable with updating. If this happens, we'll let you know and give our recommendations.)

And then we get to work with the packs . . .

Whole Enchilada Security Pack

This pack is a combination of our three individual packs for keeping your site safe and secure.

- **Updates Monitor**
- **Backup Automation**
- **Security Lockdown**

Together these packs give the technology and tools to make a Wordpress site near bulletproof. Here is a description of each:

Updates Monitor

Keeping a site up-to-date is definitely one of the more important actions as new unknown vulnerabilities are discovered. This package monitors the site for available updates to plugins, themes and core WordPress files. When updates are available, it notifies you via email.

Options:

- monitoring only active components, or all components
- frequency of checks for updates
- Which components to monitor

Backup Automation

Keeping good backups is probably the best protection against website hacking. It is near impossible to make a site 100% secure. With good backups, you know you can simply revert to an unhacked state should disaster strike. This pack will make sure you are covered.

It includes:

- Automatic backups of whole site or components you choose

- Schedule backups of desired frequency
- Choose the number of backup sets to keep (limited by available storage space)
- Easy restore of previous backup
- Site Migration Tools
- Full reports of backup
- Email notification of backup status
- Backup to remote location, including:
    - Dropbox
    - Amazon S3
    - Rackspace Cloud Files
    - Google Drive
    - FTP
    - Copy.Com
    - SFTP / SCP
    - WebDAV
    - S3-Compatible (Generic)
    - OpenStack (Swift)
    - DreamObjects
    - Email

Security Lockdown

This list is quite extensive. The most visible and obvious security measures are as follows.

- Default user and poster names
- First we look at common openings that WP users often don't know about.
    - Use of generic account names like "admin" or "administrator"
    - Using the same name for login and posting credits
- Unique login URL

    - We eliminate the default login address that every hacker knows and replace it with an address unique to the website.
- We add captcha protection to the WP login, comments and password reset.
- We set a temporary “lockout” then someone is simply trying too many passwords to get in.

Here is a full list of what we cover with the Security Lockdown, some by default, others as options:

User Accounts Security

- Detect if there is a user account which has the default "admin" username and easily change the username to a value of your choice.
- The plugin will also detect if you have any WordPress user accounts which have identical login and display names. Having account's where display name is identical to login name is bad security practice because you are making it 50% easier for hackers because they already know the login name.
- Password strength tool to allow you to create very strong passwords.

User Login Security

- Protect against "Brute Force Login Attack" with the Login Lockdown feature. Users with a certain IP address or range will be locked out of the system for a predetermined amount of time based on the configuration settings and you can also choose to be notified via email whenever somebody gets locked out due to too many login attempts.
- As the administrator you can view a list of all locked out users which are displayed in an easily readable and navigable table which also allows you to unlock individual or bulk IP addresses at the click of a button.
- Force logout of all users after a configurable time period

- Monitor/View failed login attempts which show the user's IP address, User ID/Username and Date/Time of the failed login attempt
- Monitor/View the account activity of all user accounts on your system by keeping track of the username, IP address, login date/time, and logout date/time.
- Ability to automatically lockout IP address ranges which attempt to login with an invalid username.
- Ability to see a list of all the users who are currently logged into your site.
- Allows you to specify one or more IP addresses in a special whitelist. The whitelisted IP addresses will have access to your WP login page.
- Add captcha to WordPress Login form.
- Add captcha to the forgot password form of your WP Login system.

User Registration Security

- Enable manual approval of WordPress user accounts. If your site allows people to create their own accounts via the WordPress registration form, then you can minimize SPAM or bogus registrations by manually approving each registration.
- Ability to add captcha to the WordPress user registration page to protect you from spam user registration.

Database Security

- Easily change the default WP prefix to a value of your choice with the click of a button.
- Schedule automatic backups and email notifications or make an instant DB backup whenever you want with one click.

File System Security

- Identify files or folders which have permission settings which are not secure and set the permissions to the recommend secure values with click of a button.
- Protect your PHP code by disabling file editing from the WordPress administration area.
- Easily view and monitor all host system logs from a single menu page and stay informed of any issues or problems occurring on your server so you can address them quickly.
- Prevent people from accessing the readme.html, license.txt and wp-config-sample.php files of your WordPress site.

htaccess and wp-config.php File Backup and Restore

- Easily backup your original .htaccess and wp-config.php files in case you will need to use them to restore broken functionality.
- Modify the contents of the currently active .htaccess or wp-config.php files from the admin dashboard with only a few clicks

Blacklist Functionality

- Ban users by specifying IP addresses or use a wild card to specify IP ranges.
- Ban users by specifying user agents.

Firewall Functionality

We can easily add a lot of firewall protection to your site via htaccess file. An htaccess file is processed by your web server before any other code on your site. So these firewall rules will stop malicious script(s) before it gets a chance to reach the WordPress code on your site.

- Access control facility

- Instantly activate a selection of firewall settings ranging from basic, intermediate and advanced
- Enable the famous "5G Blacklist" Firewall rules courtesy of Perishable Press
- Forbid proxy comment posting
- Disable trace and track
- Deny bad or malicious query strings
- Protect against Cross Site Scripting (XSS) by activating the comprehensive advanced character string filter. or malicious bots who do not have a special cookie in their browser. You (the site admin) will know how to set this special cookie and be able to log into your site.
- WordPress PingBack Vulnerability Protection feature. This firewall feature allows the user to prohibit access to the xmlrpc.php file in order to protect against certain vulnerabilities in the pingback functionality. This is also helpful to block bots from constantly accessing the xmlrpc.php file and wasting your server resource.
- Ability to block fake Googlebots from crawling your site.
- Ability to prevent image hotlinking. Use this to prevent others from hotlinking your images.
- Ability to log all 404 events on your site. You can also choose to automatically block IP addresses that are hitting too many 404s.

Brute force login attack prevention

- Instantly block Brute Force Login Attacks via our special Cookie-Based Brute Force Login Prevention feature. This firewall functionality will block all login attempts from people and bots.
- Ability to add a simple math captcha to the WordPress login form to fight against brute force login attacks.
- Ability to hide admin login page. Rename your WordPress login page URL so that bots and hackers cannot access your real WordPress login URL. This feature allows you to change the default login page (wp-login.php) to something you configure.

- Ability to use Login Honeypot which will helps reduce brute force login attempts by robots.

WhoIs Lookup

- Perform a WhoIs lookup of a suspicious host or IP address and get full details.

Security Scanner

- The file change detection scanner can alert you if any files have changed in your WordPress system. You can then investigate and see if that was a legitimate change or some bad code was injected.
- Database scanner feature can be used to scan your database tables. It will look for any common suspicious-looking strings, javascript and html code in some of the WordPress core tables.

Comment SPAM Security

- Monitor the most active IP addresses which persistently produce the most SPAM comments and instantly block them with the click of a button.
- Prevent comments from being submitted if it doesn't originate from your domain (this should reduce some SPAM bot comment posting on your site).
- Add a captcha to your wordpress comment form to add security against comment spam.

Front-end Text Copy Protection

- Ability to disable the right click, text selection and copy option for your front-end.

Regular updates and additions of new security features

- WordPress Security is something that evolves over time. We will be updating the All In One WP Security plugin with new security features (and fixes if required) on a regular basis so you can rest assured that your site will be on the cutting edge of security protection techniques.

Works with Most Popular WordPress Plugins

- It should work smoothly with most popular WordPress plugins.

Additional Features

- Ability to remove the WordPress Generator Meta information from the HTML source of your site.
- Ability to prevent people from accessing the readme.html, license.txt and wp-config-sample.php files
- Ability to temporarily lock down the front end of your site from general visitors while you do various backend tasks (investigate security attacks, perform site upgrades, do maintenance work etc.)
- Ability to export/import the security settings.
- Prevent other sites from displaying your content via a frame or iframe.

If you want to know more, just let me know.

GARRY DUFRESNE
206-795-5719
garry@prospermountain.com