Information Pack

This purpose of this pack is to give you a general overview of the threats that exist to a web site's security and explain how WP-Ensure solves those problems and gives you the peace of mind of knowing that your site is well taken care of.

The Problem

Digital crime has been around for as long as the internet. Stolen credit card numbers, personal information and passwords are sold on the dark side of the internet for fraud and theft purposes.

As if the criminals aren't bad enough, there are also people out there who love nothing more than the challenge of taking down a site just for the fun of it.

All this sounds very dramatic but it's important to know that hacking isn't (usually) personal, although it can certainly feel like it when your site has been attacked.

Hackers use automated software known as bots. Bots allow hackers to test many sites at the same time, to find security vulnerabilities. Once a vulnerability is found, they can exploit it to install malware, phishing sites or other malicious code.

The Solution

Read on to learn about the different kinds of site vulnerabilities and how to combat them. Hopefully, you find the information useful as a good starting point to securing your own website whether you order WP-Ensure or decide to take care of security on your own.

The Human Element

Before we get into the nitty-gritty of how WP-Ensure goes about securing your site, I would like to tell you about two of the most useful and unique features that make WP-Ensure different from other WordPress managed hosting services.

Reporting

On the first of each month you get a clear report that shows how many threats have been stopped during the previous month, actions that have been taken on your site to improve security, how many backups have been taken, how many scans have been done and other information about plugin, theme and core updates.

The feature that makes WP-Ensure unique is that during the month we are also assessing your site and writing recommendations. These recommendations are written by a real human (me!) and includes actionable information on how to improve your site. The recommendations range from technical recommendations (security, themes, plugins etc.) to search engine optimisation (webmaster tools, meta tag problems and social media tag problems).

This personal touch I believe gives you much more value for money than regular technical maintenance.

Support

You can think of our service as your own personal technical support department. If you need help using a plugin or theme, you can contact us for help.

With our service, you can build your website yourself with the comforting knowledge that we are standing in the wings should you need extra help or run into a problem.

Securing Your Website

Hosting

By far the most common threat to sites is hosting. If your website is on servers which are not updated often enough, or that are not being monitored properly then hackers can use those security holes to get into your site.

Solution: Always pick your web host carefully. Pick a large host that has lots of experience in managing sites and test their support teams to make sure they respond to queries quickly and can help should your site be compromised.

Our Solution: WP-Ensure sites are hosted on top-notch Litespeed servers, which are managed by two different companies, one in the UK and one in Finland. Server maintenance and security are best left to professional teams who enjoy and specialise in that kind of work. Partnering with high-quality hosting companies allows us to focus on maintaining website security and supporting our customers.

Website and Code Security

Sometimes your site is compromised by a plugin or theme hole that is later patched up. Even though the hole is fixed, your site is still infected. Security plugins/malware scanners and code integrity checks scan your site for issues and let you fix a hack before it becomes a problem.

Solution: Pick a good security plugin for your site. We recommend WordFence as it has a great scanner and a lot of options. There are other good ones though, such as Sucuri.

Our Solution: We run a total of three different types of daily scans on your website. One scan is internally installed on your site and checks that your plugin/theme files have not been tampered with. The second scan is from an outside scanning service checking for malware from a visitor perspective. The third is an internal server scan for malware. These scans alert us to any problems with your site quickly and stop malware from spreading out of control.

Site Hardening

Hardening your site means setting options that are known to secure your site more. Some examples are denying access to files on your installation, excluding access to xmlrpc.php and changing your databases' prefix from wp_ to a random string. These hardening steps change over time as new threats emerge.

Solution: Hardening your site requires a certain amount of technical expertise however security plugins can help you with this and are frequently updated with new options for enhanced security.

Our Solution: When moving your site to our servers, we apply site hardening and our monitoring tools to secure your site. We also check and repair basic problems such as the default wp_ database prefix.

Software Updates

Theme Vulnerabilities

Some themes use bits of code known as libraries, which do a specific job. For example, hundreds of themes might use the same PHP library to resize mages. As soon as a vulnerability is found in the library, any code using that library is vulnerable to attack.

Solution: Pick themes that are actively updated and always keep them updated.

Plugin Vulnerabilities

Plugins suffer from the same problems as themes. Developers use certain code libraries which can lead to mass exploitation. If a plugin is popular enough, and provides an incentive to hackers (for example credit card information from e-commerce plugins or user data from form plugins) it will have its own group of specialised hackers who try to take advantage of its weaknesses.

Solution: Keep plugins updated. If you're running any kind of site where user information is collected (especially e-commerce) this is an absolute must.

WordPress Core

The core of WordPress is pretty secure these days, but occasionally a threat does come up. Luckily, WordPress has a self-updating mechanism and updating WordPress has been as easy as pie for years.

Solution: Keep WordPress updated to the latest version. If you don't have time to manually check for updates, make sure auto-update at least is on for small version updates. We'd also recommend keeping a minimum of themes and plugins on the site as they need to be updated more frequently than the core.

Our Solution: WP-Ensure takes care of theme, plugin and core updates ensuring they do not break your site. When plugins or themes age or are not actively updated, we give recommendations on how to replace them to keep your site working as well as the day it was published. We uninstall dangerous themes and plugins as well and follow threats in the WordPress community to pro-actively keep your site safe.

Security Monitoring

Very few people have the time or inclination to watch what's happening on their site constantly. Security monitoring logs everything happening on a site, which can be viewed later to find out how a site has been compromised and give clues on how to fix it in the future.

Solution: Install a plugin such as Activity Log which will keep logs on what is happening on your site. There are also logging plugins which save their data to a different server/Google Drive etc, for added security.

Our Solution: We coded a custom plugin which reports activity back to our servers so that we can monitor thousands of sites efficiently. Using the data we have coded our own custom tools that search for patterns and alert us to suspicious activities. We can then change security settings and increase security as required on a site-by-site basis. One area where this has been especially effective is in stopping brute force attacks.

Brute Force Attacks

Brute attacks are login attempts from bots which are trying to guess your password. Selecting a difficult username and password is one of the most important things you can do for your site.

Solution: Your passwords should be at least 10 characters long with numbers and symbols in it. If you have trouble remembering passwords then I recommend you use a service such as LastPass.com to store them. LastPass also has a password generator so all your sites can have secure passwords and it keeps track of them.

Our Solution: As well as making sure all admins have secure passwords, the software we use is efficient in keeping brute force attacks at a minimum. If a bot tries using a username that doesn't exist such as 'admin' it will be locked out for hours. If a bot tries and fails three times to guess a password, it gets locked out for hours. Our custom tools allow us to monitor whether brute force attacks are getting more frequent (for instance if the bots are trying with real usernames) so we can tighten security on the site and firewall. The server also has its own methods of dealing with this kind of attack.

Site Backups

Many people purchase cheap hosting and assume it comes with daily backups. This is true for many hosts but one thing that's often lacking is easily accessing and restoring those backups. Unfortunately, many people don't realise they don't have fresh backups until it is too late.

Solution: Make sure that your site is properly backed up daily. Check that you can download and restore those backups quickly if required. If you are using a backup plugin on WordPress, we'd also recommend making sure it can back up to Google Drive or Dropbox, remote backups are better in case something happens to the server.

Our Solution: Your site is backed up at least once a day. Critical sites on larger WP-Ensure packages are backed up more frequently. Prevention is better than cure, so backups are very rarely required with our service, but it's still good to have them! Backup restoration is also included in our service so if your site is compromised.

WP-Ensure

We've gone through the most critical security features that are part of our service but there are a few other benefits that are included as standard such as:

- Free domain name
- Free SSL certificate and installation
- WordPress migration and installation
- Speed optimization
- Reporting
- Support

Feel free to contact us at hello@wpensure.com if you have any questions about our service and you can even book a short chat to discuss whether WP-Ensure is right for you and your website.

Diginörtti (Lisa-Marie Karvonen)

I'm a Scottish and Finnish web developer who started working in WordPress back in 2004 (yes I'm just that old). I have been running my own development company (Diginörtti FI23601001) since 2010 and serve a range of clients from one-person companies with small landing pages to large associations with thousands of sites on WordPress multisite.

I started work on WP-Ensure (known as WP-Turva in Finnish) back in 2015 when I realised that many of my customers wanted the benefits of open-source software but did not have enough time or interest to maintain it and I (of course!) loved digging into the nitty-gritty of software updates and monitoring and finding new ways to use WordPress.

Over the past four years, I have developed the WP-Ensure platform and codebase and grown the number of sites I serve as new coding projects came up. Now I am focusing on improving the service and marketing it to the best of my abilities.

Despite WP-Ensure being quite a technical challenge I also enjoy the human element of my work. I like meeting customers, I like being able to help them and with this service, I get to provide the best of both worlds, technical support but with a real human behind it :)

lisa@wpensure.com | @lisakarvonen