Securing WordPress 101

1. **Passwords, passwords, passwords**

   Brute force attacks are one of the easiest to implement.
   Everyone can crack your WordPress password just by Googling how to do that with the help of widely available software.
   Solution? Use strong password at least 10 characters long, including capital letters, numbers and special characters.
   To secure your admin access even better use **WP ShieldMate Security Plugin**.
   It adds extra layer of security to your admin login page.
   Literally no one will be able to login to your admin area even if some hacker successfully cracked their password. Check out the demo for more details:
   http://www.pluginsbyigor.com/recommends/wp-shieldmate

2. **How to know if your website got hacked and how to monitor malicious activity.**

   Install Exploit Scanner – it's a plugin that searches the files on your website, and looks in the posts and comments tables of your database for anything suspicious. It also examines your list of active plugins for unusual filenames.
   It does not remove anything. That is left to you to do which brings us to the next step.

3. **Defending against hackers.**

   Much like your computer, your website needs an antivirus:
   AntiVirus - useful plugin that will scan your theme templates for malicious injections.
   Automatically. Every day.
   Features: virus alert in the admin bar, cleaning up after plugin removal, translations into many languages, daily scan with email notifications, database tables and theme templates checks, WordPress 3.x ready: both visually and technically, whitelist solution: mark suspected cases as "no virus", manual check of template files with alerts on suspected cases, optional: google safe browsing for malware and phishing monitoring.

4. **Updating WordPress and Plugins**

   Like many modern software packages, WordPress is updated regularly to address new security issues that may arise. Improving software security is always an ongoing concern, and to that end you should always keep up to date with the latest version of WordPress. Older versions of WordPress are not maintained with security updates.

   Want to free yourself of constant new updates headache?
   In WordPress 3.7 automatic background updates were introduced in an effort to promote better security, and to streamline the update experience overall.

   By default, only minor releases – such as for maintenance and security purposes – and translation file updates are enabled.

   However you can take this one step further and also enable automatic background updates for core updates, plugin updates, theme updates, translation file updates.

Instructions for doing this are here but it requires you to know how to use FTP and to be comfortable with making small file edits.

5. **File Permissions**

File permissions are intended for securing access to certain parts of your website from unwanted people and scripts.
Most hosting providers utilize good practice of file permissions on their servers however there is room for improvements.
This step requires you to be ok with using FTP. You can find further details here.

Of course there are many other things you can do to secure your site even further but these 5 steps will give you a solid defense against 99% of attacks.

Cheers,

Igor Burban

http://www.PluginsByIgor.com