Protecting WordPress - Security Basics

Here is an outline of things you can do to help keep your installation of WordPress secure.

1. Keep Your Workstation Secure

a. Have and regularly scan your machine for viruses or malicious software.
b. Update your browsers, anti-virus, and operating system regularly.
c. Install security patches as soon as they become available.
d. Use a firewall, at the router and the ISP level if possible.
e. Update local passwords often, at least every 2-3 months.

2. Use Strong Passwords

a. http://www.pcmag.com/article2/0,2817,2368484,00.asp
b. It is so important to get this one right, no excuses.
c. Don’t share your password.
d. Don’t use the same password in multiple locations.
e. Avoid the mindset that someone isn’t going to hack you.

3. Protect wp-admin users

a. Rename the admin user to something unique, but know that your username is published in a variety of locations on your website. Just renaming the admin user may not necessarily protect your account.
b. Make sure that each admin user on your account has a secure and unique password.
c. Yubikey is an additional option that can further secure your login, check out the details for that here: http://www.yubico.com/

4. Keep WordPress and other applications updated

a. These updates fix bugs, close security holes, and add functionality.
b. The most important part of updating is patching known security issues, as hackers will scan for particular versions of WordPress and attempt to crack in with these known vulnerabilities.
c. Do the same for any themes or plugins you have installed – updates are vital to account security.
d. If you worry about themes or plugins being broken with updates, you need to utilize different themes or plugins – the providers of these addons should be keeping up with the WordPress updates to keep users like you as secure and functional as possible.
e. If you’re not a developer you should look at plugins/themes with paid update or support options, as these will be more likely to help keep your website secure.

5. Do not look like a “new” WordPress installation

a. Remove default posts, etc.
b. Remove “Powered by WordPress” footers
c. Remove install or upgrade files
i. Be sure to delete /wp-admin/install.php and /wp-admin/upgrade.php after every WordPress installation or upgrade.
ii. You don’t need them for day to day WordPress functionality.
d. Change some of the misc default settings
i. Go to Settings > Miscellaneous in your admin console and change the names of wp-content/directory and wp-comments-post.php.
ii. Make sure to change the template URL within the template and wp-comments-post.php accordingly, to maintain the function of your site.

For further information, refer to our Advanced WordPress Security article.

Also, you may find these links helpful:

http://codex.wordpress.org/FAQ_Security
http://codex.wordpress.org/Hardening_WordPress
http://wordpress.org/extend/plugins/limit-login-attempts/

Related articles

- Optimised Wordpress Hosting
- How Do I Cancel
- How Do I Restore My Account From A Backup
- Two Factor Authentication Security - 2FA
- How To Upgrade A Shared Hosting Package