WordPress Security Briefing

Notes and links

How to Tell if Your Site Has Been Hacked

- Google Site Operator - go to google.com and search “site:yourdomainname.com” - This search returns a list of all of hte pages on your site that Google has indexed. You’re looking for unexpected content in your page descriptions. On a hacked site you may see references to Viagra and other pharmaceuticals.
- Google Safe Browsing Diagnostics Use this URL to see a Google report on your domain (be sure to change domainname.com): http://www.google.com/safebrowsing/diagnostic?site=yourdomain.com
- Google Webmasters Tools Setup your account and add each of your website domains. Google will notify you when they detect Malware. Webmaster Tools can also be used to identify a range of other problems that may impact your ranking in Google.
- Sucuri.net Proactively scan your site for malware. Securi support plans include daily scanning and site repair.

Have a Good Backup Plan in Place

- Backup your site regularly. Schedule database backups daily, and full site backups weekly. More frequently if you’re making more regular changes to your site. Be sure that your backups are moved to a secure location off of your web server. If your engaged in ecommerce or any sort of user-based transactions (membership sites, etc.) consider a real-time backup service like VaultPress.
- You’ll find more information on disaster and recovery planning here: Preparing for a WordPress Disaster.
- BackupBuddy - WordPress backup software.

WordPress Setup Tips

- When installing WordPress be sure to:
    1. Use a secure password
    2. Don't use the name 'admin' or any variation
    3. Set the database prefix to something other than "wp_"

  while #2 and #3 can be fixed after installation, doing so requires a plugin like Better WP Security, listed below.
- Double check folder permissions after installation. Install the ServerBuddy plugin to check permissions and PHP server settings (in your WordPress Admin go to Plugins -> Add New - and then search for ServerBuddy).

User Account Security

- Create a special user account for posting. Give that account an Editor role. User accounts with Administrative privileges should only be used when performing administrative tasks.
- Use a secure password (the built-in WP password strength meter is a useful benchmark on password strength).
- Don't re-use passwords. Use a program like 1Password to manage password for all of the sites you login to regularly.

WordPress Updates & Maintenance

- Install WordPress updates as soon as possible after they become available.
- Install Plugin and Theme updates as soon as they become available.
- Delete any unused themes and plugins. Both can make your site vulnerable even if they aren't activated. This video and worksheet will give you some guidelines to use when determining which plugins are really needed and which can be safely deleted: WordPress Disaster Planning
- If you have multiple WordPress installations consider using a service like ManageWP or an application like InfiniteWP to manage your sites.
- Delete any themes or plugins you aren't using. The one exception is the parent theme (if you're using a child theme). If a child theme is active and it depends on the Parent theme which will be listed under Available Themes (installed, but not active). Never delete the parent theme - the child theme won't work on it's own. Most child themes will say "child theme" in the description under "Current Theme." For more information on sorting out which plugins you really need and which can be safely deleted watch How to Solve the WordPress Plugin Paradox.
- Better WP Security is something of a Swiss Army knife for WP security. It's available from the WordPress plugin directory and can be installed from the Admin plugin menu. You can use this plugin to limit login attempts, change the admin user name, change your database prefix and more. Caution: Be sure to do a full site backup before using this plugin.

— Block Bad Traffic & Speed-Up Your Website —

- CloudFlare is a security service that blocks malicious Internet traffic and speeds up your website. It's free for most sites.

Presented by WPApprentice.com