WordPress Security Checklist

As the owner of a web development firm (Callkayla.com), we are constantly hearing about client sites being hacked. If this hasn't happened to you, it very well could sooner than later if you don't take the necessary precautions. While hackers will continue to devise methods to infiltrate blogs and websites, the following steps will help keep your WordPress Site safe.

1. I've removed telltale signs that give hackers a clue about my site including:
   - ☐ The WordPress version from the website's header – don't tell people what version of WordPress you are running, especially if your version isn't up to date.
   - ☐ Remove your admin user name and replace it with a unique user name and password.
   - ☐ Remove login link from my theme.

2. I've secured my login and installed plug-ins and systems that do one or more of the following:
   - ☐ Limit the number of login attempts an IP address can use within a specific timeframe.
   - ☐ Add two-factor authentication, which will require you to enter an additional code to login.
   - ☐ Renamed the "wp-login.php" file to something else (such as "log-in.php") so that hackers cannot know the correct login URL.

3. I've added SSL for my WordPress Admin. (Note: You will need to contact your web host to have them implement a Secure Socket Layer for your WordPress Admin area.

4. I've established systems to:

   - ☐ Scan my site regularly for virus and malware
   - ☐ Update plug-ins and WordPress software
   - ☐ Back-up my WordPress site regularly

5. I've created a strong password to log into my site. It includes upper and lower case letters, numbers and special characters. My password has nothing to do with me or my personal life, so it cannot be guessed, and I have a system to change it at least once every 90 days.

6. I utilize reputable and trustworthy providers including:

   - ☐ Website designers/developers
   - ☐ WordPress Theme developers
   - ☐ Ghost/Guest bloggers
   - ☐ Virtual assistants, and
   - ☐ Each provider is given a unique password and username and administrative login information is changed after business with provider(s) is concluded.

7. I've changed the default table prefix in the WordPress database, or had it changed for me, so that hackers cannot easily access my database. (Note: For a new WordPress installation, you can change the table prefix in the "wp-config.php" file before installing WordPress. If you have WordPress installed, visit WordPress.org for instructions.)

8. I've uninstalled and removed any and all unnecessary themes, plug-ins, and users.

9. I've employed the services of a reputable host with demonstrated security practices and systems in place and a reputation for secure hosting.

10. I've created systems to ensure my back-up system is working effectively and efficiently. Backing up your WordPress site isn't a "set it and forget it" event. Create a system to regularly check to make sure your blog/site is backing up effectively.

No blog or website is impervious to hackers. However, when you take these ten steps to protect your site, you're drastically reducing your odds of trouble. It's well worth the time and effort up front to protect your business down the road.