My clients are asking me what they receive for their website(s) hosting fee which is $119.40 per year. I have included a complete list below. If you are interested please read on and let me know if I can answer any of your questions.

The list below works on my servers to keep your website(s) from being hacked and up to date. There is no guarantee that keeps all websites safe from intruders, however I do everything I can to prevent it.

Maintenance:

Maintenance for all of the WordPress sites on my servers is an ongoing process. This does not include any Maintenance agreement for changes on your site. That is a separate agreement for design and copy changes to you website and does not include any of the items listed below.

1. Making sure all websites are running the most current version of WordPress.
2. Always making sure plug-ins are updated.
3. Running WordPress scans automatically on a daily basis.
4. Consistently updating a WordPress theme when possible. This depends on what theme is installed. On any new site this is not a problem. If I inherit a site that is running an older less stable WordPress theme on located another server problems can occur.
5. Making backups of all sites with a plugin called WP Clone. This plug-in creates a cloned backup of your website in case of a server malfunction, hack, or other unforeseen problem that might bring a site down

Security measures for all sites currently on my servers:

I have over 150 websites that are running on my servers plus I am the admin for 75 other sites that are not on located on my servers. Hostgator is my hosting provider of choice. Hostgator is ranked #4 out of 10 in PC Magazines the Best Web Hosting Services for 2020. I use Hostgator because it is WordPress friendly and does offer a high level of security tools for my sites.

One of my main concerns is a Brute Force Attack. Unlike hacks that focus on vulnerabilities in software, a Brute Force Attack aims at being the simplest kind of method to gain access to a site: it tries usernames and passwords, over and over again, until it gets in.

Another way in to a WordPress site is through an exploit from a plugin. The vast majority of account compromises are caused by malicious users who have found exploits in scripts installed on an account. With all WordPress installations I have a step by step process that has worked well up to date. I have not had a security breech with any of my WordPress websites located on my servers.

I use a very solid responsive WordPress theme called Divi from Elegant Themes for all of my sites. The foundation of this theme is solid.

Installation of Wordfence. Wordfence is a plugin that fights off scraper attempts, aggressive robots, fake bots, unauthorized login attempts, and even strong brute force attacks.

Wordfence Security Features:

1. Fully IPv6 compatible including all whois lookup, location, blocking and security functions.
2. Includes support for other major plug-ins and themes like WooCommerce.
3. Real-time blocking of known attackers. If Wordfence is attacked and blocks the attacker, your site is automatically protected.
4. Scans for the HeartBleed.
5. Enforces strong passwords among your administrators, publishers and users.
6. Scans core files, themes and plug-ins against WordPress.org repository versions to check their integrity.
7. Includes a firewall to block common security threats like fake Googlebots, malicious scans from hackers and botnets.
8. Blocks entire malicious networks. Includes advanced IP and Domain WHOIS to report malicious IP's or networks and block entire networks using the firewall.
9. See how files have changed. Optionally repair changed files that are security threats.
10. Scans for signatures of over 44,000 known malware variants that are known security threats.
11. Scans for many known backdoors that create security holes including C99, R57, RootShell, Crystal Shell, Matamu, Cybershell, W4cking, Sniper, Predator, Jackal, Phantasma, GFS, Dive, Dx and many many more.
12. Continuously scans for malware and phishing URL's including all URL's on the Google Safe Browsing List in all your comments, posts and files that are security threats.
13. Scans for heuristics of backdoors, trojans, suspicious code and other security issues.
14. Checks the strength of all user and admin passwords to enhance login security.
15. Monitors your DNS security for unauthorized DNS changes.
16. Rates limits or blocks security threats like aggressive crawlers, scrapers and bots doing security scans for vulnerabilities in your site.

17. Includes login security to lock out brute force hacks and to stop WordPress from revealing info that will compromise security.
18. Monitors disk space which is related to security because many DDoS attacks attempt to consume all disk space to create denial of service.