

SiteLock, CodeGuard, And Other Bluehost Add-Ons: Decide Now

Bluehost offers several add-ons like SiteLock and CodeGuard, each addressing specific website needs. This document helps you decide whether these add-ons are necessary for your situation. We'll cover functionality, alternatives, and practical decision-making steps.

[Get 60% OFF on Bluehost Hosting →](#)

Understanding SiteLock

SiteLock is a website security tool that scans for malware and vulnerabilities.

It offers features like daily scans, vulnerability patches, and a web application firewall (WAF).

Consider SiteLock if you handle sensitive user data or run an e-commerce site. Otherwise, free alternatives might suffice.

Assessing CodeGuard

CodeGuard provides automated website backups and version control.

It backs up your website files and databases daily, allowing you to restore to previous versions.

Evaluate your comfort level with manual backups. If you prefer automation and easy restores, CodeGuard is helpful.

Making Your Decision

- Step 1: Identify your security and backup needs.
- Step 2: Research free or lower-cost alternatives (e.g., Wordfence, UpdraftPlus).
- Step 3: Compare the features and pricing of Bluehost add-ons with alternatives.
- Step 4: Test alternatives before committing to a paid add-on.

Consider the cost of your time spent managing backups and security manually.

Alternatives and Considerations

For security, explore free security plugins like Wordfence or Sucuri Security.

For backups, consider plugins like UpdraftPlus or BackupBuddy. These often offer free and paid options.

Regularly update your CMS (e.g., WordPress), themes, and plugins to minimize vulnerabilities. cPanel -> WordPress -> Updates.

Strong passwords and two-factor authentication are crucial regardless of add-ons.

Implement a web application firewall (WAF) through Cloudflare's free plan for basic protection.

Example .htaccess rule to block suspicious IPs:

```
<Limit GET POST PUT>
order allow,deny
deny from 123.45.67.89
allow from all
</Limit>
```

Example command to manually backup MySQL database:

```
mysqldump -u [username] -p[password] [database_name] > backup.sql
```

Examples

- WordPress Dashboard -> Plugins -> Add New: Search for 'Wordfence' to install a security plugin.
- cPanel -> File Manager: Navigate to your website's root directory to manually download backup files.
- Cloudflare Dashboard -> Security -> WAF: Configure basic firewall rules to protect your site.
- Example: To check if a file exists on your server via SSH: `ls -l /path/to/your/file`

Tips

- Regularly back up your website, even if you don't use CodeGuard.
- Keep your CMS and plugins updated to prevent security breaches.
- Implement strong passwords and two-factor authentication for all accounts.
- Monitor your website's traffic for suspicious activity.

[Get Started With Bluehost — Launch Your Site in Minutes →](#)

FAQ

Q: Do I really need SiteLock if I have a small website?

A: Not necessarily. If you keep your software updated and use strong passwords, free security plugins and a WAF might be sufficient. Regularly scan your site with online tools.

Q: How often should I back up my website?

A: At least weekly, or daily if you frequently update your content. Test your backups regularly to ensure they are working correctly.

Q: Can I use both a security plugin and SiteLock?

A: Yes, but be mindful of potential conflicts. Monitor your website's performance and error logs after enabling both. Often, one well-configured solution is better than two conflicting ones.

This document is for informational purposes only. It is not official and is not affiliated with or endorsed by Bluehost. Information provided here may be outdated and should not be considered professional advice. This document may contain affiliate links.