How To Secure A cPanel Account From Hackers

This article is for cPanel Accounts. Determine where your account is with this guide.

In an effort to help improve the security on the servers we encourage clients to follow some of our best practices. Please keep your contact information current and up to date in cPanel. This is critical to receive important information and critical updates. We also ask that you keep your site applications current and up to date with the latest versions when possible. Doing these simple tasks will not only help you but it will help us as we continue to work to provide you with the best hosting experience possible.

As another reminder for the future, here are 9 security tips our admins highly recommend:

1. Make sure that you have up to date Spyware / Malware / Anti Virus protection on any computer that connects to the site via FTP and SSH. Run a scan on these machines and fix whatever issues arise.

2. Once the above step is done, Change all FTP user account passwords. Make sure the passwords you reset are secure. Use upper and lower case lettering and numbers.

3. Make sure that allow_url_include, fopen, and register_globals are set to “off” within any customized php.ini files you have within your account.. Also make sure you have included insecure functions within the disable_functions list. This only applies if you are running PHP applications within your account.

4. Update any applications you are running to the latest stable versions. Newer versions will contain security patches for known exploits within that application. This also applies to any 3rd party plugins you are running for these applications.

5. Search the internet for ways to further secure these applications. There are usually quite a few extra steps you can take.

6. Keep an eye on files within your account, pay attention to files that aren’t yours, recently modified files etc. These can be indications of malicious content. Remove any malicious content found.

7. Make frequent personal backups, and make sure that your backups are not infected with malicious code. That way you can easily restore files if you need to.

8. Check all administrative areas of your sites. Make sure they are all password protected. Sometimes hackers remove this protection which can lead to easy entry later.

9. Check your applications for new Administrative user accounts that hackers may have setup as back doors. Remove any and all suspicious user accounts.