



Cyber-attacks are an unfortunate reality of the digital age. As information becomes increasingly accessible, so do opportunities for cyber attackers to steal your data. These attacks have caused major disruptions in many businesses and put valuable data at risk.

In a shared hosting environment, you may be wondering how to identify and prevent these attacks.

It is crucial for businesses set up in a shared hosting environment to know how they can identify and prevent these attacks.

This post will take you through the steps you can take to identify and prevent a cyber-attack for shared hosting.

How to Prevent Cyber Attacks In A Shared Hosting Environment

Once you have identified that your website has been under a cyber-attack, it's time to start working on ways to prevent future attacks.

Implementing security measures against cyberattacks on a shared hosting environment is challenging as all the hosting accounts running on nameservers may be using different CMS.

Different hosting accounts may also be using varied security configurations and services, which may prevent you from implementing water-tight security measures.



There are also steps you can take to help prevent cyberattacks in a shared hosting environment.

Implement 2 Factor Authentication

2Fa authentication is a great security measure that will help to prevent unauthorized access to your website. It also provides enough protection against brute force attacks.

While it's not always an option for shared hosting environments, implementing 2-factor authentication will help you keep your website safe.

You should have Google Authenticator (or any other smartphone app) installed on all devices used by the people who manage your site.

Install Website Security Plugins

Security plugins installed on your website offer services that protect you from DDoS attacks, malware infection, spamming, phishing, and more.

Security plugins like Wordfence and Sucuri are the best options if you're looking for plugins that offer malware scanning, spam protection, firewall installation, and more.

Block PHP Execution in Unknown Folders

Hackers can exploit vulnerabilities on your website to add folders and files to your directory.



This is done so that the hacker can upload malicious code onto your site and take control of it.

Ensure that you block PHP execution in unknown folders to help protect against exploitation by hackers. You can use plugins such as MalCare to block unknown PHP execution automatically. You can also learn more about [how to block PHP execution manually](#).

Perform Website Vulnerability Scans

Website vulnerability scans will identify vulnerabilities and security flaws on your website.

Vulnerability scans are an important part of cyberattack prevention. They help you in knowing what to prioritize before hackers take advantage of the vulnerabilities.

Depending on how often you update your plugins, you should perform a scan every month or at least once per quarter.

The best options for website vulnerability scans are a paid option like Sucuri SiteCheck or the free option from Mozilla AMP Validator. You can also use Google's Vulnerability Scanner to identify vulnerabilities on your site and fix those issues before hackers exploit them.

Install Web Application Firewalls

The most effective way of preventing DDoS attacks from bringing your business down is by distributing your resources to multiple locations. That way, it will be difficult for attackers to target your whole business.

It's also important that you monitor your website traffic and have an accurate idea of how your website traffic looks like on a typical day. This will help you spot DDoS attacks early enough and mitigate the problem before it cripples your services.

Use Advanced Security Measures

A VPN can often be used in a shared hosting environment as it protects you and other websites on the same server against malicious intruders.

You can also use SSL certificates, CSP or Content-Security-Policy (CSP), code signing, and other security measures to protect your website from cyberattacks.

Update Your Web applications, Plugins, and Themes

It's important to update your web applications, plugins, and themes as soon as new patches are released.

This is because newer versions may include security fixes that can help protect you against cyberattacks. It's also worth checking for any updates from the plugin or theme providers before updating so you have all of the latest bug fixes included in the update.

Review Your Hosting Options

Reviewing your hosting options is important as it helps you find a web host that offers the best protection against cyberattacks.

You can search for different hosts and compare their features, pricing plans, and level of security on offer by conducting research online. This will help you to choose which web host provides the right levels of protection for your website.

Reduce Your Risk of Being Hacked

A full website backup is essential to reducing your risk of being hacked. You should always back up your site so that you can restore it in case the worst happens and someone hacks into it.

This will allow you to minimize the impact on your business when a hack takes place and ensure that you can recover any data lost.

While it's hard to manage the security of a website under a shared hosting environment, implementing multiple security measures can help you prevent an attack on your website. Ensure that you stay up to date with the latest updates and security measures to keep your website safe.

References

<https://www.malcare.com/blog/shared-hosting-security/>



<https://bitninja.io/blog/how-to-identify-and-prevent-cyberattacks-in-a-shared-hosting-environment/>

<https://preyproject.com/blog/en/what-are-cyber-threats-how-they-affect-you-what-to-do-about-them/>

<https://www.firewall.cx/general-topics-reviews/security-articles/1092-security-tips-how-to-protect-your-websites-and-webservers-from-hackers.html>