

WHAT TO LOOK FOR IN GOOD SECURE HOSTING





Having a website is the best way to promote your business online. But, it's not enough to have a website. You also need secure web hosting for people to trust your website and use it safely.

It can be difficult to know what features are important in good secure web hosting so that your website can stay safe from attackers.

This article will discuss what to look for in good secure web hosting and how to find a reputable and reliable web hosting company.

What is Secure Hosting?

The web hosting company and the type of web hosting you use are necessary for keeping your website safe and secure.

Secure web hosting involves a collection of stand-alone factors optimized to ensure that your website is hosted securely.

Secure web hosting plays a primary role in ensuring that your website is safe from malicious intrusions and attacks.

A secure web host makes use of multiple security layers and high-level encryption on different components of your website to prevent unauthorized access to your website.



It's therefore important that you find a reliable company when shopping for website hosting.

Must-Have Security Features on Secure WebHosts

When looking for a good secure web hosting company, there are a few features that you should look for:

1. Malware and virus protection
2. Data encryption
3. Firewall protection
4. DDoS Protection
5. Secure DNS
6. Antispam and antiphishing tools
7. Web application firewall
8. Domain Name Privacy

FireWalls

firewall is software that can detect intrusions and stop them before they reach your site.

Firewalls work by filtering all request activities before they reach the webserver. They can then block access to your website based on set security criteria.



Firewalls in secure web hosts are designed to protect from various threats that come in over the internet.

It can also detect and stop malicious traffic from impacting your website's performance or crippling it with a denial of service attack (DoS).

A dedicated firewall is a service where specific rules are set for who should/shouldn't access your website. Dedicated firewalls are essential for websites that process sensitive information.

Antispam and Antiphishing Tools

Antispam tools in secure web hosting are tools that help to reduce the amount of spam that is sent to your website and can also detect any malicious emails.

Antiphishing tools in secure web hosting prevent your website from being used to host phishing websites.

Antispam helps identify and block spam messages, while antiphishing identifies phishing websites trying to steal your data.

An excellent secure web hosting company will have antispam and antiphishing tools in place to stop your website from being used for illegal purposes or hacked.

Web Application Firewall

Web application firewalls are a form of firewall explicitly designed to protect applications running on a server. Web application firewalls filter requests to your website and can detect any suspicious activity.

A good secure web hosting company will have a firewall in place to protect your website from malicious intrusion or attack.

When you buy domain privacy, it means that the WHOIS information for your domain is hidden.

Domain name privacy hides your personal information and contact details from the public. This is an important feature to have for any website that handles sensitive information.

Good secure web hosting providers will offer domain name privacy as a service to protect your business's private data from cybercriminals who might try and steal it or use it against you in some way.

DDoS Protection

DDoS is a type of attack that aims to make your website unavailable by overwhelming it with requests.



When a server receives a big load of requests, it can't respond to any of them and becomes 'overwhelmed'.

DDoS attacks are usually triggered by a botnet. A network of computers that have been infected with malware or other malicious software without their owner's knowledge.

To prevent DDoS attacks, secure web hosting companies work with Content Delivery Networks such as Cloudflare.

Antivirus Protection

Secure websites require antivirus software for malware, viruses, or other infections on the server platform (such as Unix or Linux).

Availability and Uptime

One of the most important things to look for in a website hosting company is its availability and uptime.

Availability means that they have enough server resources when you need them, so your site won't go down under heavy traffic or any other circumstances.

Uptime refers to how much time the servers are available each day (or year).



A good hosting company will have a 99.99% uptime, but this can vary depending on the server platform and use of resources.

Backup and Restoration

Secure web hosting providers that offer backup and restoration services will have the ability to restore your website in case of an outage.

Backups are important as they can help you recover from any data loss due to a server crash.

A good secure web hosting company will have backups and restoration in place to recover your website quickly should anything happen.

In conclusion, it's important that you find a dependable website hosting company that you can trust to keep your website up and running. Ensure that the company you choose has the right security measures in place, has a proven uptime and availability record, and can restore your website in case of any data loss.

References

<https://www.theslstore.com/blog/7-security-factors-to-consider-when-choosing-a-web-host/>

<https://digital.com/web-hosting/secure/>

<https://www.thoughtco.com/web-hosting-requirements-3470852>