With recent digital explosion in the last decade spread all over the globe, cyber threats have become a close reality for small and big organizations. Just like any other business operation, hosting a website has become a challenging job. Moreover, there’s even a higher potential of facing threats if your website is a source of monetization for your business.

Many small businesses are under the false notion that they cannot come under the radar of cybercriminals due to their size. The limited resources they have, they try to utilize them elsewhere and consider security as secondary. However, it is this vulnerability that makes small businesses an easy target for data breaches. Though cyber attackers generally spend more resources and time on targets with high-value due to a potential of larger profits, ignoring cyber threats and giving up on preventing them because you are a small business with limited resources is a mistake.

Let’s have a look at some of the web hosting security best practices that all businesses must follow as a baseline to protect against web security threats regardless of their size.

1. **Choose a Web Hosting Provider with Established Reputation**

Your web hosting service provider has a very important role towards your website security, from the physical space of your website to the traffic that goes in and out of it. For instance, often it’s the web hosting provider that manages standard items such as anti-malware, anti-spam or even automated backup and recovery systems.

Depending upon your web host, shared hosting can sometimes get risky. If you have a number of websites registered with the same account and accessible from the same FTP, even one of them getting infected with malware will compromise all other websites.

Hence, when choosing a web host, always consider security as a primary factor. If you have the resources and reason to move to a VPS account, get it done whenever possible. This is because VPS hosting offers [increased security](https://www.bluehost.com/blog/shared-vs-vps-hosting-which-option-is-best-for-you/?utm_source=google&utm_medium=genericsearch&gclid=EAIaIQobChMIg_vr9-jt7gIVyYBQBh1TggBWEAAYASAAEgJflvD_BwE&gclsrc=aw.ds) features in comparison with standard shared hosting services.

1. **Use a Content Delivery Network**

A Content Delivery Network or CDN is a geographically distributed network of data centers and proxy servers. A CDN can serve visitors to your web pages faster by hosting your site caches on proxy servers all over the world. Whenever your site access is requested, the CDN serves cached data from the location that is closest to the location from where the request was made.

Other than the advantage of fast service, a CDN also enables load balancing by utilizing the server networks. In other words, your website can manage a large number of visitors at one point of time. Hence, it also allows the prevention of Distributed Denial of Service (DDoS) attacks. As DDoS attacks aim to shut down a website’s server by flooding it with unlimited requests, CDNs are designed to avoid these attacks by distributing the traffic through its network of servers.

1. **Use SSL Certificates**

A Secure Sockets Layer (SSL) certificate secures any information shared by visitors on your website, such as their [credit card](http://www.cardzgroup.com/products.html) or bank details. It encrypts sensitive information and has become an important standard, especially for Ecommerce websites. Major internet browsers now warn the visitors if a website is not using SSL. SSL certificates are free to install if you have a personal website or even a small business. Even for larger companies, SSL certificates are easy to obtain and install. Many web hosts now [offer this service](https://www.websitebuilderexpert.com/web-hosting/ssl/) and enable easy installation of SSL certificates.

1. **Always Create a Backup**

Although there are many web hosts that have features such as backup and restore, many of them still don’t. Regardless of this, it is always a safe practice to do your own backup and keep a set of files and database offline. Doing this manually may be a tedious task. Hence, it’s recommended to automate the process, which is easier than what one may think. If you are using WordPress, you may want to check out some of [these](https://10web.io/blog/most-reliable-wordpress-backup-service/) automatic backup services.

1. **Strengthen Your Passwords**

This cannot be stressed enough. From your personal emails and work logins to website credentials, keeping strong passwords is a basic security requirement. An easy-to-remember password is a recipe for disaster. Hackers today have access to lists of commonly used passwords that they use against a website’s defense.

To make this more understandable, cybercriminals use botnets to launch brute-force attacks that can try six-character passwords for many hours. Since botnets are automated, hence, while you and the hackers sleep, they are trying to break into your website.

To keep strong passwords, follow all [best practices](https://www.it.ucsb.edu/secure-compute-research-environment-user-guide/password-best-practices), never keep the same password twice and preferably use a password management tool.

1. **Encrypt Your Connection**

Being a website’s owner, your must secure your connection with your web hosting account. It is always recommended to transfer files either through a Virtual Private Network (VPN) connection or via a Secure File Transfer Protocol (SFTP). Either of these two methods can help prevent intruders from attempting to intercept and steal your data that is going to the web server. Though VPNs cost a bit higher than an SFTP client, they are more secure as they encrypt all the information being sent from your computer. However, if you don’t want a VPN, you can choose from many [free SFTP clients](https://www.thegeekstuff.com/2011/06/windows-sftp-scp-clients/) that are available for use.

1. **Keep Applications and Plugins Updated**

When selecting an application or plugin for a website, you need to consider its age and amounts of updates required. This enables you to know whether a software is active or not. An inactive software can have numerous security flaws. Hence, you only need to install plugins and software from reliable sources to keep away from potential malware infections.

Vulnerabilities in software are one of the easiest targets of exploitation by hackers. Almost all software programs have bugs of some kind and this is why they are regularly updated with patches to cover these loopholes. Hence, whenever possible, keep all the software programs of your website updated.

1. **Manage Server Configuration Files**

Depending upon your web hosting platform, you will have to deal with different types of server configuration files. For instance, Microsoft uses web.config files while Apache uses .htaccess. These configuration files are used for enhancing the security of your website. By managing your server configuration files, you can prevent others from browsing your directory and stop them from hotlinking to images on your website.

You can find which web server you are on by clicking [here](https://sitecheck.sucuri.net/).

1. **Be Careful About File Permissions**

Files have different properties that define what a user can do with them, depending upon their role as owners, public or groups. File permissions include being able to read, write or execute. For optimal security, you must know about your important files and what permissions each of them has. A sensitive file with permission to public can allow anyone to access it, add malicious code to it and harm your website.

1. **Use Two-Factor Authentication**

Even if you have the longest or strongest of passwords, they can still get cracked. To add an extra layer of security, you may add two-factor authentication so the system checks your identity twice before allowing you access. The most common and quickest 2FA method is authenticating via a mobile code or the Google Authenticator.

1. **Operating Systems**

Based on your website’s technical requirements, you can choose between Linux-based OS or Windows-based OS for your web server. In terms of security, both operating systems have their own security advantages. A windows-based web server limits access by default and users need to take permission before they can be granted privileges by an administrator. On the other hand, Linux web servers have fewer threats since it is not used as widely as windows. In an event where a vulnerability is detected, the open-source Linux community often responds faster to fix the issue.

**Key Takeaways**

Although web hosting security is challenging, webmasters who are vigilant and choose a good hosting service can run their websites without undergoing a major disruption. Following basic rules like enforcing strong passwords with two-factor authentication, scheduling regular updates, getting services from trusted hosting service providers and keeping backups, your website should do just fine.