

A SIMPLE GUIDE TO WEBSITE SECURITY- 2021 BEST PRACTICES





Are you worried that you could lose your website to hackers or viruses, and other types of malware?

This article will discuss how to improve your website security by making it more difficult for attackers to hack and corrupt your website with malware or steal sensitive information from a database on your website.

It is essential that you know what your website security "weaknesses" are so that you can take action to resolve them.

Developing good security practices for your website will give you a greater sense of confidence and peace of mind. It will help a lot in reducing the risk of a potential security incident.

If you are in charge of maintaining your website, here is some advice on how to improve your website's security.

How to Improve Your Website Security

A secure website is one that has no vulnerabilities that an attacker could exploit.

A vulnerability is a weakness in the design or implementation of a website that an attacker could exploit to cause harm to you, your website, or its users.



Here are some basic steps that you can take to improve the security of your website right now.

1. Add HTTPS And SSL Certificate

The first step to securing your website is through securing your URL.

A secure URL ensures that communication between your website and the end-user on a browser is encrypted.

To secure your website URL, you will need to switch the URL from HTTP to HTTPS.

HTTPS (Hypertext Transfer Protocol Secure) is the protocol that transfers data between your website and the user over the internet securely.

To switch your site from using HTTP to HTTPS, you only need to install an SSL certificate which can be done without any coding knowledge or tools.

2. Change Your Login Credentials Regularly

The second (yet most important) thing you should do is change your website login credentials.

To start with, use a username that's not easy to guess. Avoid using the username "admin," or your first name.



Hackers can easily get your first name as it's the default name that receives the authorship attribute for all your blog posts.

Also, use a smart password that uses a combination of alphabetical, numerical, and special characters. Avoid using personal information such as your birth date.

Change your passwords regularly to make it hard for hackers to guess what the current password is.

3. Keep Your Website Clean

Databases, applications, and plugins can provide backdoors that hackers can use to gain access to your website.

Make sure that you keep your website safe by regularly cleaning files, databases, plugins, and applications that you no longer use.

Make sure that you only use plugins and applications from trusted companies.

Scanning your server and website for security vulnerabilities is also important. Security scans should be scheduled and automatic whenever there is a change to any component of your website.

4. Use a Secure Host

Think of your website as an entry to a directory. Your web host is the person who keeps that directory for people to use.

Make sure that your web host provides the right security features to keep your uploaded data safe.

Some of the indicators for a good website host include;

1. Provision of a Secure File Transfer Protocol (SFTP)
2. Security features such as 1-click backup, brute force protection, Rootkit scanner, and regular security upgrades

5. Backup Your Website Regularly

Creating regular backups is one of the best ways to ensure that your website remains safe.

Backups ensure that you can easily recover your website in case your website files are corrupted, damaged, or deleted maliciously/ unintentionally.

Make sure that you use an offsite storage location for your website data (i.e., not on the same server as your website)

6. Use Available Website Security Solutions

Make use of website security companies and plugins that offer free and paid web security solutions. A quick search on the best website security plugins will give you all the options that you can use right now to keep your website safe and secure.

Conclusion

Being a little hands-on could actually help to prevent irreparable harm and damage to your website.

While you might not have the budget to hire a website security expert, this guide is a sure resource for keeping your website secure.