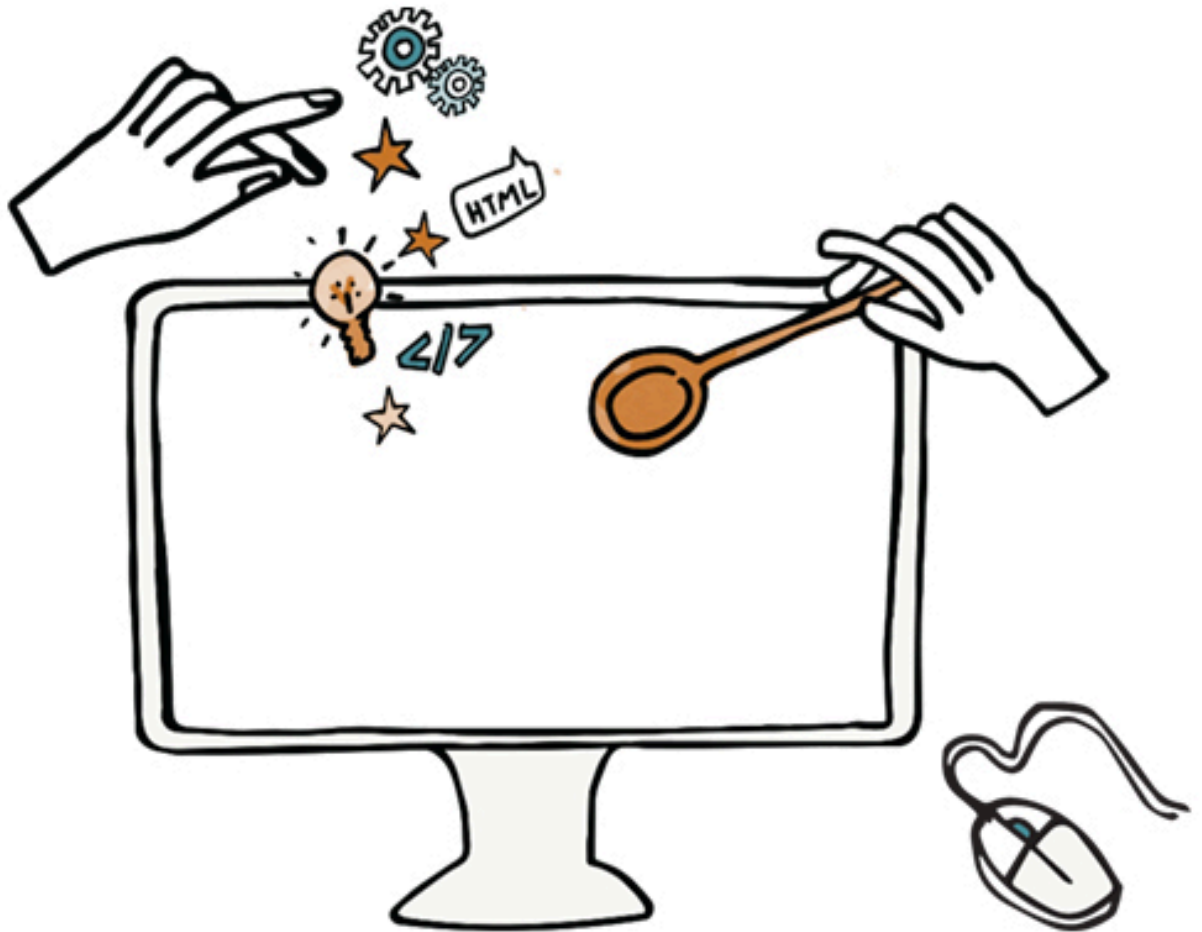


# THE Website Chef



## Hosting Guide

# Hosting Guide

---

Ingredients for a successful hosting environment.

## 1. Hosting

Your website is a collection of files that must be stored on a publicly available server. Hosting companies offer you space on their servers (shared hosting) for a fee. Depending on your business, the size of your site and the traffic to the site you may want to invest a little more than the basic hosting to store your files on a business server (often called business hosting) where the number of other websites is limited. This makes sure your site has the resources to load quickly for your customers.

## 2. How to choose a hosting company

I look for hosting companies in the country where my main customers are and who also have local technical support.

Important factors to consider:

How much disk space will be allocated to you.

## 3. SSL

SSL (Secure Socket Layer) provides a level of protection for visitors to your site in the case that they enter any information such as an email address to sign up for your mailing list or purchasing a product. The SSL certificate encrypts the data they enter so that no third party can intercept it.

Google, king of search, announced in 2018 that they were going to give priority in search results to sites that have an SSL certificate. You can tell if a site has an SSL certificate because their url (web address) will begin with https. Sites without SSL will be http. You may also see a green padlock next to a url with an SSL certificate. Even if you don't collect email addresses or sell anything it's a good idea to have the certificate as browsers like Chrome and Firefox will alert visitors to your site if you don't have one that the site is not secure.

There are several options for SSL certificates but basically you want to choose a domain-verified or organization-verified certificate. The domain-verified certificate will probably be sufficient for most businesses. It means that the certificate issuing company verified that the domain is valid.

The SSL certificate is an annual cost that you pay to your hosting company.

# Hosting Guide

---

## 4. Firewall

Unfortunately there is a lot of malicious activity on the web. To keep your website protected from being infected with malware (malicious software), viruses or hacked you can purchase a firewall that essentially puts a wall between your site and hackers.

This is an annual cost that you pay to your hosting company.

## 5. Backup Options

Hosts often offer a backup system for an extra fee. These usually will backup your site on a daily basis. This might be helpful for e-commerce sites where there is a lot of activity. Read the fine print carefully to make sure you understand what you're paying for.

## 6. External Storage Space

I recommend having an external backup option. You can have a backup taken of your site on a schedule that suits the type of activity on your site. These backups can be automatically sent to an external storage service like Amazon S3 or Dropbox. You'll want to keep at least a month's worth of backups.

## 7. Register Your Web Address (Domain)

You can register the domain by going to the website of any domain registry such as DreamHost, Name.com and Name Cheap or any hosting company you choose. You don't have to register the domain at your hosting company.

Registering the domain is an annual cost that you pay to the domain registrar you choose. Make sure you don't forget to renew or you risk losing your domain.

When you register the domain you will usually be offered an add-on service called domain privacy. ICANN is a central database of domains and contact information for said domains all around the world. Anyone can search for a domain and find out who registered the domain and where it's hosted at <https://lookup.icann.org/>. Most registrars offer domain privacy as a way to protect your contact information from the general public. You don't have to take the offer but for the small fee it may be worth it not to get inundated with emails about your domain (most of which are spam or phishing emails).