
# **http://** vs. **https://**

What does making your domain 'resolve' to https:// actually do and NOT do when triggered by installing the Auto SSL Certificate (free version) on your server?

Firstly to be awarded any SSL certificate, your domain name must be shown to have accurate records of ownership.

That means when you registered your domain name, you entered verifiable information such as:

- an actual person
- an actual address
- any further records such as an ABN if required such as if you have a .com.au domain name

This then shows your domain name was not acquired by a non-human, and the website is *less likely* to be risky. The browser Chrome, is now checking which websites do not have an SSL certificate and noting that in search results. Not only should an SSL certificate show https:// at the front of your domain name, but you will also have a green padlock as well.

This Auto SSL certificate is free, and DOES NOT protect your visitors if your website allows payments ON THE WEBSITE itself. For that you need to buy a more specific SSL certificate for encrypting sensitive information such as Credit Card details. None of my clients need this as they all use Third Party websites for any payment information entered (such as PayPal) or Bookeo.

When a website resolves (automatically shows) as a https:// - website information is encrypted (not the content that is visible) but sensitive information such as owner details, logins, any payment information, etc. Any hacker/spammer trying to access website information is presented with an encrypted version. Most robots will then move on to an easier target.

**Email**

https:// does NOT directly secure your email, nor protect you from spam or email phishing attacks. The only email protection from having a https:// domain name, comes from the fact that it's much harder for some kind of robot/malware to access your *website* information (logins, passwords etc), which could then have a flow-on effect to your email if the robot is programmed to proceed to hacking email accounts once they have already access your website.


**It is therefore highly important you protect yourself EVERY DAY, at home.**
**Install and RUN a malware/spyware protection and registry cleaner EVERY DAY such as:**

**http://www.superantispyware.com/download.html**

**AND**

**https://www.ccleaner.com/ccleaner/download**

They have free versions you can run today/right now!

- Most people don't realise a new computer doesn't always come with an excellent virus/malware program. And it may only run for 30 days or not at all unless you do something to trigger it. They also need updating, upgrading and renewing...
  Make sure they are set to “always on” and “monitoring 24/7”, and check that regularly

- Have something that cleans your browser history/cookies every time you close your browser

- REMOVE those ticks that allow programs to piggy back a download when you are downloading something you DO want

- Check your “see which programs are installed on my computer” area and remove anything you don't use any more of that you DID NOT download purposely (*be careful – make sure you **know** what you are removing*)
  Usually found under “control panel” and then “programs and features”

If you want help we can work on this, and set you up to be 99% free from “I wish I had done this earlier” moments.

Believe me, they suck!