**How HTTPS improves security over HTTP**

**HTTP** stand for Hyper Text Transfer Protocol and **HTTPS** stand for Hyper Text Transfer Protocol Secure. HTTPS makes your connection to a website more secured compared to HTTP. With HTTPS, data is encrypted in both directions: going to and coming from the origin server. HTTPS encrypts your information, like password, credit card, or personal details when you send it to the website.

When we type the name of any website in the browser and press enter. So, with HTTPS a **data layer** is created between the client and the server which protects the data from hackers. HTTPS ensures that no one can change the information as it travels between you and the website. If someone tries to mess with it, the connection will be broken, so the data remains intact. In some cases, he gets the data, but the data is encrypted, so he can't see the original data. Thus HTTPS protects our data from unauthorized access.

**HTTPS** checks that the website you are visiting is the real one, not a fake or copy trying to steal your data.

To set up HTTPS on a website, we can purchase an **SSL** (Secure Socket Layer) certificate from a trusted provider like GoDaddy and install it on our server.

In short, **HTTPS** protects your information from being stolen, making it much more secure than **HTTP**.