**HTTP** is Hyper Text Transfer protocol that is used in networking. Whenever basically you type a website in the browser, its is this protocol which by default listens at port 80 on server side and helps you to see the webpage on your machine.

**HTTP** is a application layer protocol and uses TCP as a underlying protocol for communicating and making connections. As I said it uses default port 80 for communication.

**Drawbacks of HTTP**:Http comes with some security concerns, like privacy is not there, anyone can see your content. Integrity is not there, so someone can easily alter with the content. HTTP is insecure as there's no encryption methods for it. So, it's subjected towards man in the middle and eavesdropping of sensitive information. There's no authentication, so you will not have any clear idea with whom you are initiating a communication. Authentication is sent in the clear, anyone who intercepts the request and can know the username and passwords being used.

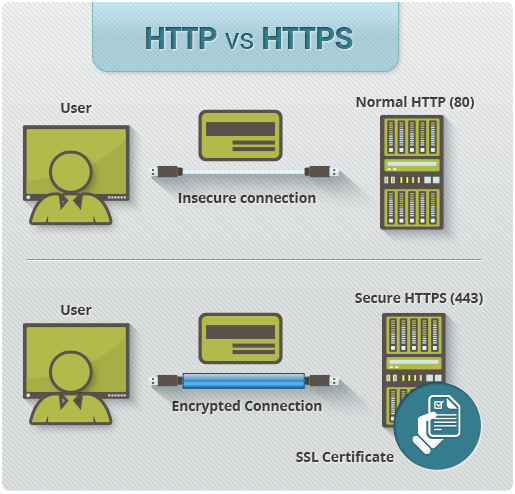
**HTTPS** : This is Hyper text Transfer protocol with added security layer in place in form on TLS/SSL. Servers and clients communicate with each other exactly same as HTTP but over a secure channel.

The SSL layer serves for two main purpose :

1) It is confirmed after using HTTPS that you are talking to server directly that you are thinking of.

2) It also ensures that only server reads the data you sent over network. No else can read it.

Here’s the basic **advantage** of using HTTPS based secured connections,



* **Authenticity**: It guarantees the user that whatever data they are provided from the website they are visiting is genuine enough to trust and has not been altered by anyone.
* **Confidentiality**: It assures users that all the activity done on the website by them is totally encrypted with HTTPS and its secured enough that it cannot be visible to someone who is trying to sniff through network traffic.
* **Protection**: It's really crucial that when someone is doing any monetary transaction such as purchasing through e-commerce website, visitor want to stay assured that their confidential information such as credit card or bank details stay secured and do not fall into wrong hands, and this HTTPS based URL does the same thing, it assures users that its completely safe enough to do transactions.

The **disadvantages**:

* **Performance**  
  When a transaction is initiated on a site with SSL certificate, the process involves encryption and decryption of the data transferred mutually. Because of this, the connection slows down. However, a small sacrifice in speed is worth the extra security. The SSL certificate service provider should make sure the process encrypts and decrypts information in real-time.
* **Cost**  
  Getting a SSL certificate for your business can be expensive because the service providers need to pay for maintenance of the infrastructure and they have to verify your business credentials. All this entails cost. Therefore, it may not be a viable option for small businesses.
* **Expired certificate**  
  You need to renew your SSL certificate periodically. When it expires, customers visiting your site get a pop-up message saying that the SSL certificate in your site has expired, and the site is not secure any longer.  
  If you do not renew the SSL certificate, you are likely to lose customers' trust.

**In conclusion:**

A SSL certificate is good for your business because it protects your customers' data, protects the credibility of your business, and it is likely to help you build a good brand image in the long run.