Secure Communications (HTTPS) –

This basically says that your connection is basically secure, we have to understand different benefits that we get from https,

* Data Encryption –

It gives you data encryption what it meant by, it ensure the data which is getting transferred from your client to the server in between these the data is unreadable even if you are try to access the data you wont be able to understand what kind of data it basically going because it not readable data transferred from the server.

* Authentication –

There is a certificate when there is a client to server connection is setup, a certificate is basically provided to the client and that certificate is actually used for all the communication or for encryption that happen, that certificate is provided by certificate authorities basically we call as SSL OR TLS basically certificate that we have.

Now how this certificate basically helps – consider example the certificate that your server is basically providing, in case that certificate is not valid or expired your browser basically or client is able to understand the things which is coming is not secure is not valid and it show warnings and it wont basically accept, it says boss you have to check and rectify your certificate.

* Data Integrity –

It ensures the data that you are sending is not manipulated in between how internally when the data is getting transferred it uses cryptographic encryption or the checksum basically to ensure that the data getting transferred is not tempered, so there is checksum validation that happens on the client and the server basically where if the data is tempered then it will get to know, the data is getting tempered I am not going to use that. It uses something called mac (message authentication code) that is what we use.

* Protection against Phishing –

To hack and make a duplicate of a website and that looks exactly similar to that, having a https is a rare and if someone do not have a https website then you will get to know ohh boss there is something which is not right because all the website are from good provider they uses https and if it is not having those then please do not trust them and do not use them that brings first level security.

* Data Privacy –

The data which goes from client to the server in between no one basically steel the data or loop into what is going to happen example, we talked about isp provider.

The data transfer which is happening it cannot be tracked in between those layers.

* Compliance with Security Standards –

There are multiple Compliances which says that we have to use the https if you don’t use I am not going to provide.

* Trust and Reputation –

As you say if I have a website which is normal http website and I have a website which is not https website which shows a green colour lock kind of things.

* Search Engine Ranking –

If you have a website which is http and if you have a website which is https the content of https will have more search engine ranking as compare to http more the secure the more the better search engine ranking basically has.

* Protection Against Browser Warnings –

In case as we talked about the certificate expired many of the website many of the browser if the website is http or do not have the right certificate all of these it show the warning.

* Faster website loading –

Now the other thing is faster website loading, to use http2 protocol you have to use https protocol.