



Topic: HTTP & HTTPS

Hypertext Transfer Protocol (HTTP) and Hypertext Transfer Protocol Secure (HTTPS) are two protocols used for transferring data over the internet.

HTTP is the foundation of data communication on the World Wide Web, and it defines the rules for how web browsers and web servers communicate with each other. When you visit a website using HTTP, your web browser sends a request to the web server, and the server responds with the requested data, such as a web page or a file.

However, HTTP is not secure, and data transmitted using HTTP is vulnerable to interception and tampering. To address this issue, HTTPS was developed as a more secure version of HTTP. HTTPS adds a layer of security by using SSL/TLS encryption to protect data in transit, making it more difficult for attackers to intercept and access sensitive information.

When you visit a website using HTTPS, your web browser establishes a secure connection to the web server, and all data exchanged between the two is encrypted. This ensures that any data that is intercepted is unreadable and protected from tampering. HTTPS is particularly important for websites that handle sensitive data, such as online banking, e-commerce sites, and social media platforms.

In summary, HTTP is used for transferring data between web browsers and web servers, while HTTPS adds an additional layer of security by encrypting the data in transit. HTTPS is essential for protecting sensitive information and ensuring the security of online transactions and communications.

