



HTTP VS HTTPS





HTTP and HTTPS are two protocols used for communication between web browsers and servers.

Let's compare them and understand why HTTPS is crucial for a secure browsing experience.

Swipe -->



Due to security concerns, there's a push to migrate from HTTP to HTTPS.

Search engines prioritize HTTPS sites, and browser warnings discourage HTTP usage.



HTTP (Hypertext Transfer Protocol)

HTTP transmits data between browsers and servers without encryption.

It's fast and suitable for general browsing but lacks security measures.



HTTPS (Hypertext Transfer Protocol Secure)

HTTPS extends HTTP with encryption for secure communication.

It protects sensitive data from eavesdropping and ensures data integrity.



Security

HTTP is vulnerable to attacks like data interception and tampering.

HTTPS encrypts data, making it unreadable to unauthorized parties.



Data Privacy

HTTP doesn't provide data privacy, making it risky for transmitting sensitive information.

HTTPS encrypts data, safeguarding user privacy.



Authentication

HTTP doesn't validate server identity, making it susceptible to impersonation attacks.

HTTPS uses digital certificates to authenticate servers.



Trust and Credibility

HTTPS displays a padlock icon and "https://" in the address bar, assuring users of a secure connection.

It enhances trust and credibility.



**Follow if you found
this valuable.**

