HTTPS

Hypertext Transfer Protocol Secure or HTTPS is an extension of the HTTP protocol. HTTPS secures the data transfer between client and server by encrypting all of the communication.

HTTPS allows a client to safely share sensitive information with the server through an HTTP request, such as credit card information, passwords, or bank account numbers.

Security and Encryption

HTTPS requires that the client use https://developer.mozilla.org/en-US/docs/Glossary/SSL or TLS to protect requests and traffic by encrypting the information in the request. HTTPS is just HTTP with extra security!
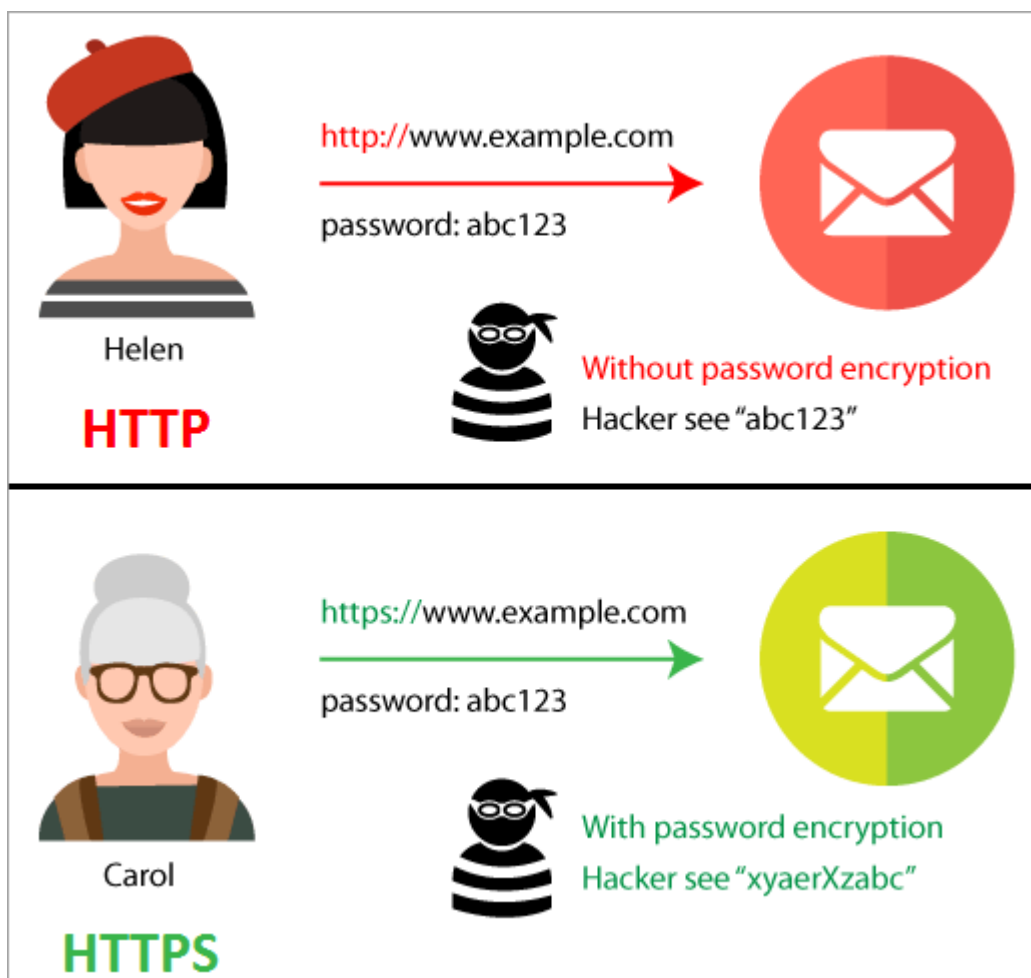
HTTPS keeps your messages private, but not your identity

We won't cover how encryption works in this course, but we will in later courses! For now, it's important to note that while HTTPS encrypts what you are saying, it doesn't necessarily protect who you are. Tools like VPNs are needed for added privacy.

HTTPS ensures that you're talking to the right person (or server)

In addition to encrypting the information within a request, HTTPS uses digital signatures to prove that you're communicating with the server that you think you are. If a hacker were to intercept an HTTPS request by

tapping into a network cable, they wouldn't be able to successfully pretend they are your bank's web server.