First and foremost, an SSL certificate acts as visual confirmation to users that our website is a safe and secure environment, with encryption in place to prevent attacks.

Have you ever noticed that some URLs start with http://, while others start with https://?

Where'd that extra "s" come from, and what does it mean?
To put it simply, the extra "s" means your connection to that website is secure and any data you enter is safely shared with that website. The technology that powers that little "s" is called SSL, which stands for "Secure Sockets Layer."

SSL is security technology. It's a protocol for servers and web browsers that makes sure that data passed between the two are private.

It does this using an SSL Certificate. This certificate is a digital certificate that authenticates the identity of a website and encrypts information you send to the server using SSL technology. Encryption is the process of scrambling data into an undecipherable format that can only be returned to a readable format with the proper decryption key.

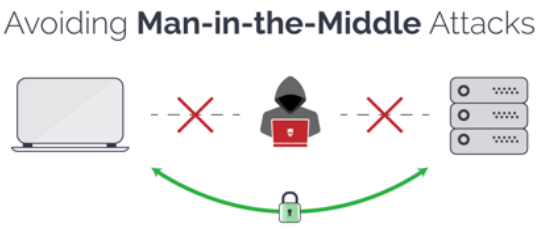
A certificate serves as an electronic passport that establishes an online entity's credentials when doing business on the Web. When an Internet user attempts to send confidential information to a Web server, the user's browser accesses the server's digital certificate and establishes a secure connection.

Typically, an SSL certificate contains the following information:

- The certificate holder's name
- The certificate's serial number and expiration date
- A copy of the certificate holder's public key
- The digital signature of the certificate-issuing authority

Why do we need it?
When you land on a page which is *unsecure* and you fill in a form and submit it, the information you enter can be intercepted by a hacker.

This information could be anything from details on a bank transaction to an email registering for an offer. In hacker lingo, this "interception" is often referred to as a *"man-in-the-middle attack"*



If you're wondering how attacks happen, here's one of the most common ways.

A hacker places a small, undetected listening program on the server hosting a website.

That program waits in the background until a visitor starts typing information on the website, and it will activate to start capturing the information and then send it back to the hacker.

A little scary, right?

But when you visit a website that's encrypted with SSL, your browser will form a connection with the web server, look at the SSL certificate, then bind your browser and the server. This binding connection is secure to ensure no one besides you and the website can see or access what you type.

This connection happens instantly, and in fact, some suggest it's faster than connecting to an unsecure website. You simply have to visit a website with SSL, and *voila* — your connection will automatically be secured.

When you're online, you always want to see https:// when visiting any site that you choose to trust with your essential information.