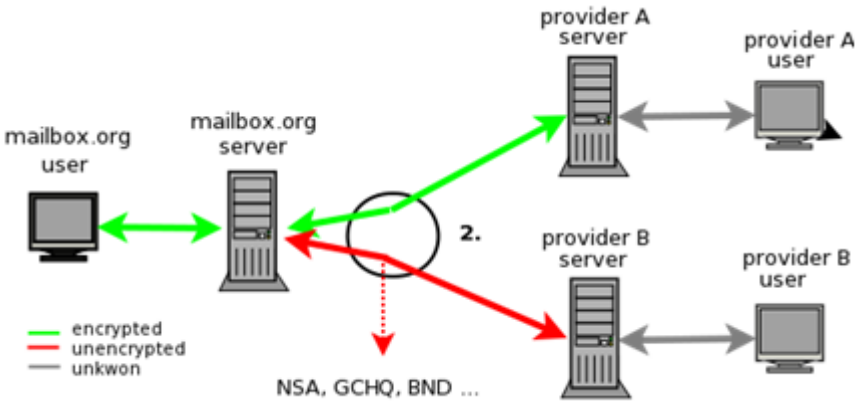
About SSL

Do you think web security is important? How can we keep secure while we are surfing the internet? Today, we will talk about something about web security.

What are SSL and TLS?

Secure Sockets Layer (SSL) is a security protocol that provides privacy, authentication, and integrity to Internet communications. SSL eventually evolved into Transport Layer Security (TLS).

TLS, the successor of the now deprecated SSL, is a cryptographic protocol designed to provide communications security over a computer network. Several versions of the protocol are widely used in applications such as email, instant messaging, and voice over IP, but its use as the Security layer in HTTPS remains the most publicly visible.



https://kb.mailbox.org/display/MBOKBEN/SSL-TLS+encryption+at+mailbox.org

The SSL/TLS protocol encrypts internet traffic of all types, making secure internet communication (and therefore internet commerce) possible. Here are the basics of how it works and what comes next.

What is an SSL certificate?

SSL certificate, as the description in the previous section made clear, these certificates are at the heart of the SSL/TLS protocol: they provide the client with the public cryptographic key necessary to initiate secure connections. But their purpose goes beyond just supplying the key itself; they also authenticate that the key is in fact associated with the organization offering it to the client.

TLS vs. SSL

When the next version of the protocol was released in 1999, it was standardized by the Internet Engineering Task Force (IETF) and given a new name: *Transport Layer Security,* or TLS. As the TLS specification notes, "the differences between this protocol and SSL 3.0 are not dramatic." Thus, it's not really a matter of TLS vs. SSL; rather, the two form a continuously updated series of protocols and are often lumped together as SSL/TLS.

The TLS protocol encrypts internet traffic of all types. The most common is web traffic; you know your browser is connected via TLS if the URL in your address starts with "https," and there's an indicator with a padlock telling you the connection is secure, as in this screenshot from Chrome:

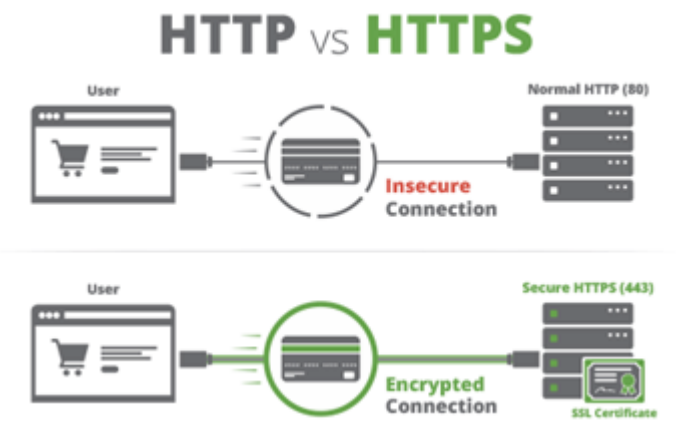
But TLS can be used by other applications as well, including e-mail and Usenet.

Why is HTTP not secure? | HTTP vs. HTTPS

HTTP requests and responses are sent in plaintext, which means that anyone can read them. HTTPS corrects this problem by using TLS/SSL encryption.

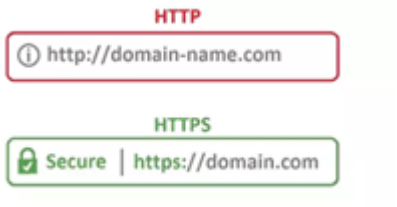
Google.com

HTTP vs. HTTPS: What are the differences?



Google.com

HTTPS is HTTP with encryption. The only difference between the two protocols is that HTTPS uses TLS (SSL) to encrypt normal HTTP requests and responses. As a result, HTTPS is far more secure than HTTP. A website that uses HTTP has http:// in its URL, while a website that uses HTTPS has https://.



Google.com

So, now we know the concepts of SSL, TLS, HTTP, and HTTPS, and I hope it might help you keeping your security while you connect to the internet website.

1. https://en.wikipedia.org/wiki/HTTPS
2. https://en.wikipedia.org/w/index.php?title=Secure_Sockets_Layer&redirect=no
3. https://en.wikipedia.org/wiki/Transport_Layer_Security#SSL_1.0,_2.0,_and_3.0
4. https://www.csoonline.com/article/3246212/what-is-ssl-tls-and-how-this-encryption-protocol-works.html
5. https://www.websecurity.digicert.com/security-topics/what-is-ssl-tls-https
6. https://www.cloudflare.com/