



# What Is HTTPS?

HTTPS is a secure way to send data between a web server and a web browser.

What is SSL? ☐

What is an SSL Certificate? ☐

What is TLS? ☐

Why Use HTTPS? ☐

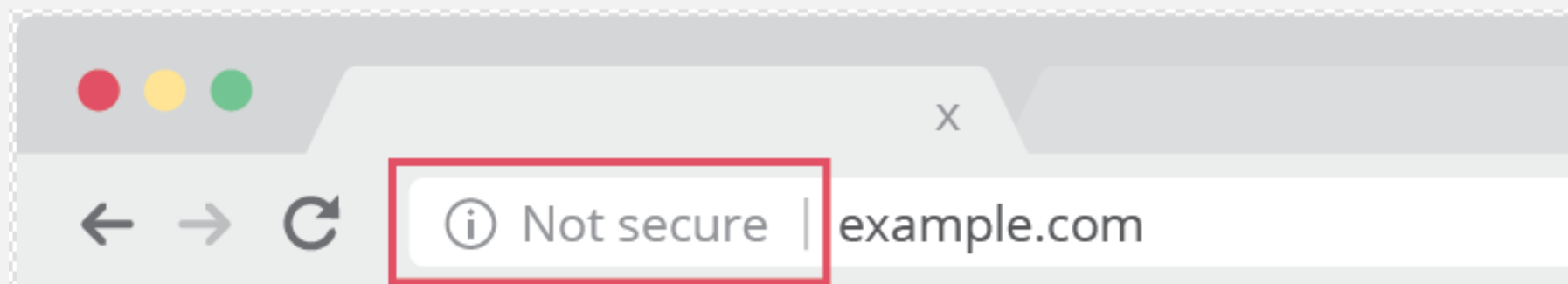
What is HTTPS? ☐

## What is HTTPS?

Hypertext transfer protocol secure (HTTPS) is the secure version of [HTTP](#), which is the primary protocol used to send data between a web browser and a website. HTTPS is encrypted in order to increase security of data transfer. This is particularly important when users transmit



browsers take HTTPS seriously; [Google Chrome and other browsers flag all non-HTTPS websites as not secure.](#)



You can use the [Cloudflare Diagnostic Center](#) to check if a website is using HTTPS.

## How does HTTPS work?

HTTPS uses an encryption protocol to encrypt communications. The protocol is called Transport Layer Security (TLS), although formerly it was known as Secure Sockets Layer (SSL). This protocol secures communications by using what's known as an asymmetric public key infrastructure. This type of security system uses two different keys to encrypt communications between two parties:

1. The private key - this key is controlled by the owner of a website and it's kept, as the reader may have speculated, private. This key lives on a web server and is used to decrypt information encrypted by the public key.
2. The public key - this key is available to everyone who wants to interact with the server in a way that's secure. Information that's encrypted by the public key can only be decrypted by the private key.

## Why is HTTPS important? What happens if a website doesn't have HTTPS?



communications that occur over HTTP occur in plaintext, making them highly accessible to anyone that has access to the network, and vulnerable to [on-path attacks](#).

With HTTPS, traffic is encrypted such that even if the packets are sniffed or otherwise intercepted, they will come across as nonsensical characters. Let's look at an example:

### Before encryption:

This is a string of text that is completely readable

### After encryption:

ITM0IRyiEhVpa6VnKyExMiEgNveroyWBP1gGyfkf1YjDaaFf/Kn3bo30fghBPDWo6AfSH1ntL8N7ITEwIXc1gU5X73xMsJormzzXlw0yrCs+9XCPk63Y+z0=

In websites without HTTPS, it is possible for Internet service providers (ISPs) or other intermediaries to inject content into webpages without the approval of the website owner. This commonly takes the form of advertising, where an ISP looking to increase revenue injects paid advertising into the webpages of their customers. Unsurprisingly, when this occurs, the profits for the advertisements and the quality control of those advertisements are in no way shared with the website owner. HTTPS eliminates the ability of unmoderated third parties to inject advertising into web content.



# Stanford University



MENU

You can close this overlay in 3 seconds.

MYHABIT

PRECIOUS METALS

UP TO 60% OFF JEWELRY

JOIN NOW >

100 YEARS OF KNOWLEDGE and researchers.

changing needs of students



close

AT&T Digital Life and you.  
*Bringing it all home  
for our customers.*

A photograph of a man in a blue polo shirt standing in a room with a fireplace and framed pictures.



technically speaking, HTTPS is not a separate protocol from HTTP. It is simply using TLS/SSL encryption over the HTTP protocol. HTTPS occurs based upon the transmission of [TLS/SSL certificates](#), which verify that a particular provider is who they say they are.

When a user connects to a webpage, the webpage will send over its SSL certificate which contains the public key necessary to start the secure session. The two computers, the client and the server, then go through a process called an SSL/TLS handshake, which is a series of back-and-forth communications used to establish a secure connection. To take a deeper dive into encryption and the SSL/TLS handshake, [read about what happens in a TLS handshake](#).

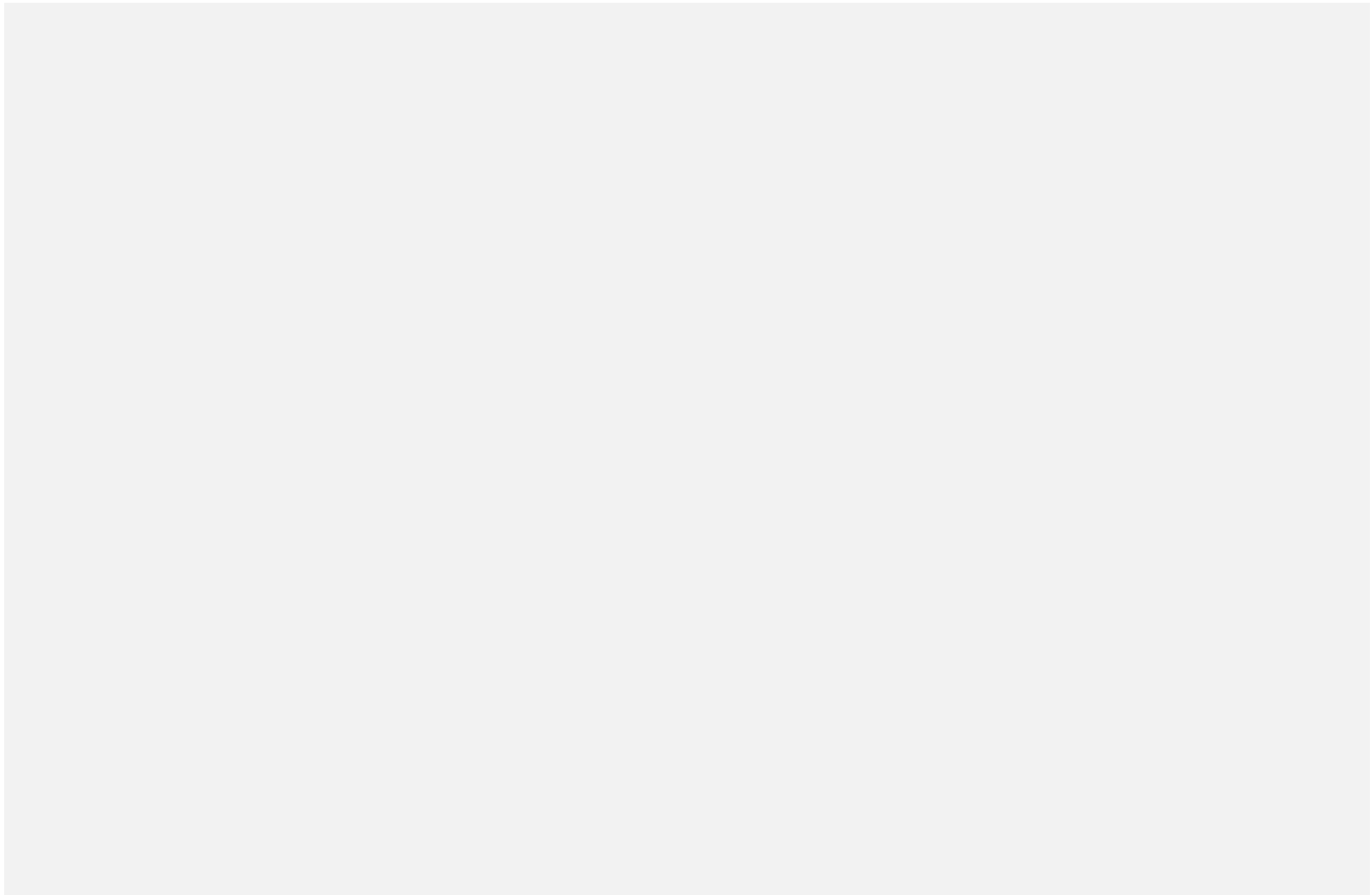
## How does a website start using HTTPS?

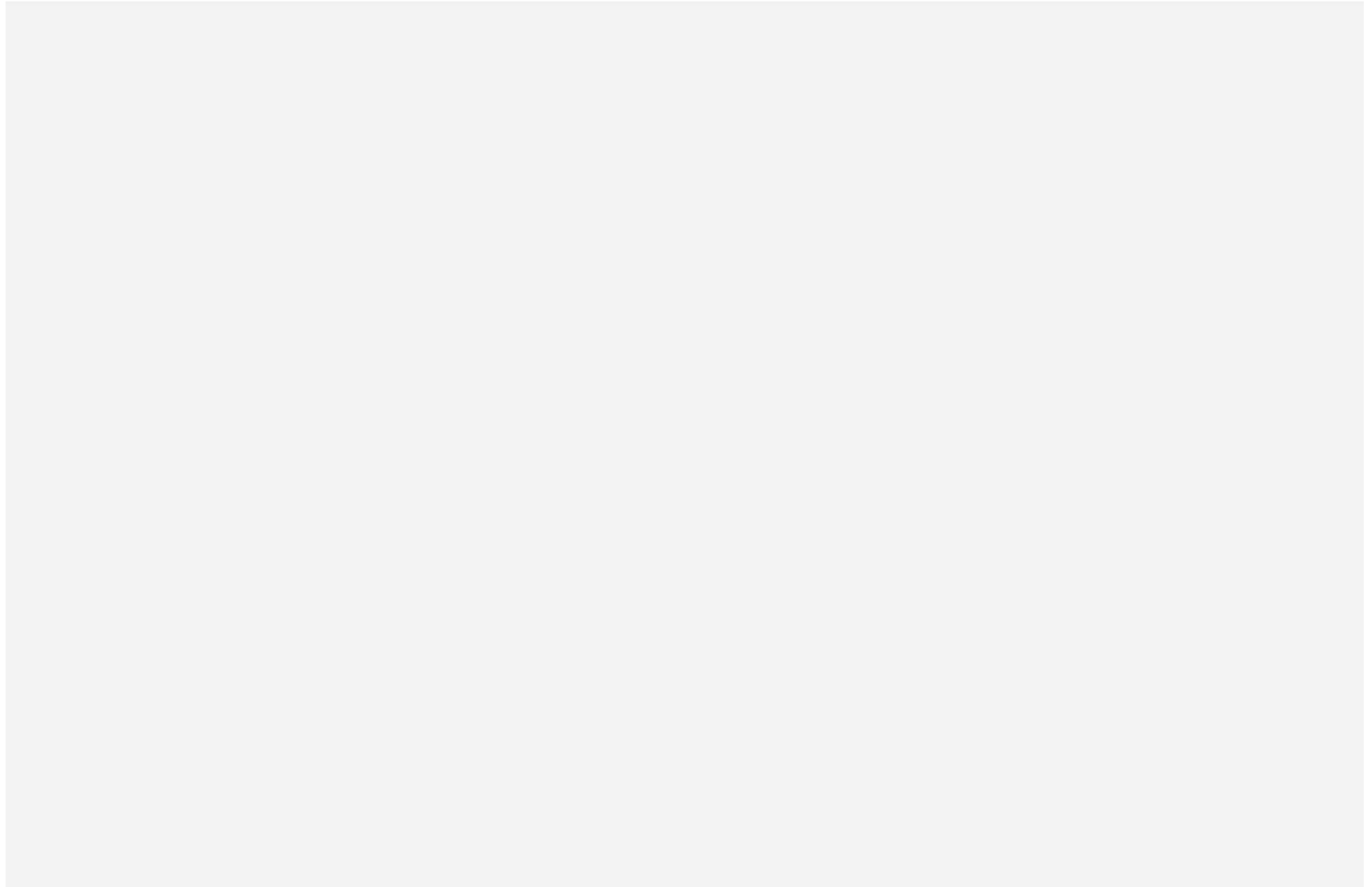
Many website hosting providers and other services will offer TLS/SSL certificates for a fee. These certificates will be often be shared amongst many customers. More expensive certificates are available which can be individually registered to particular web properties.

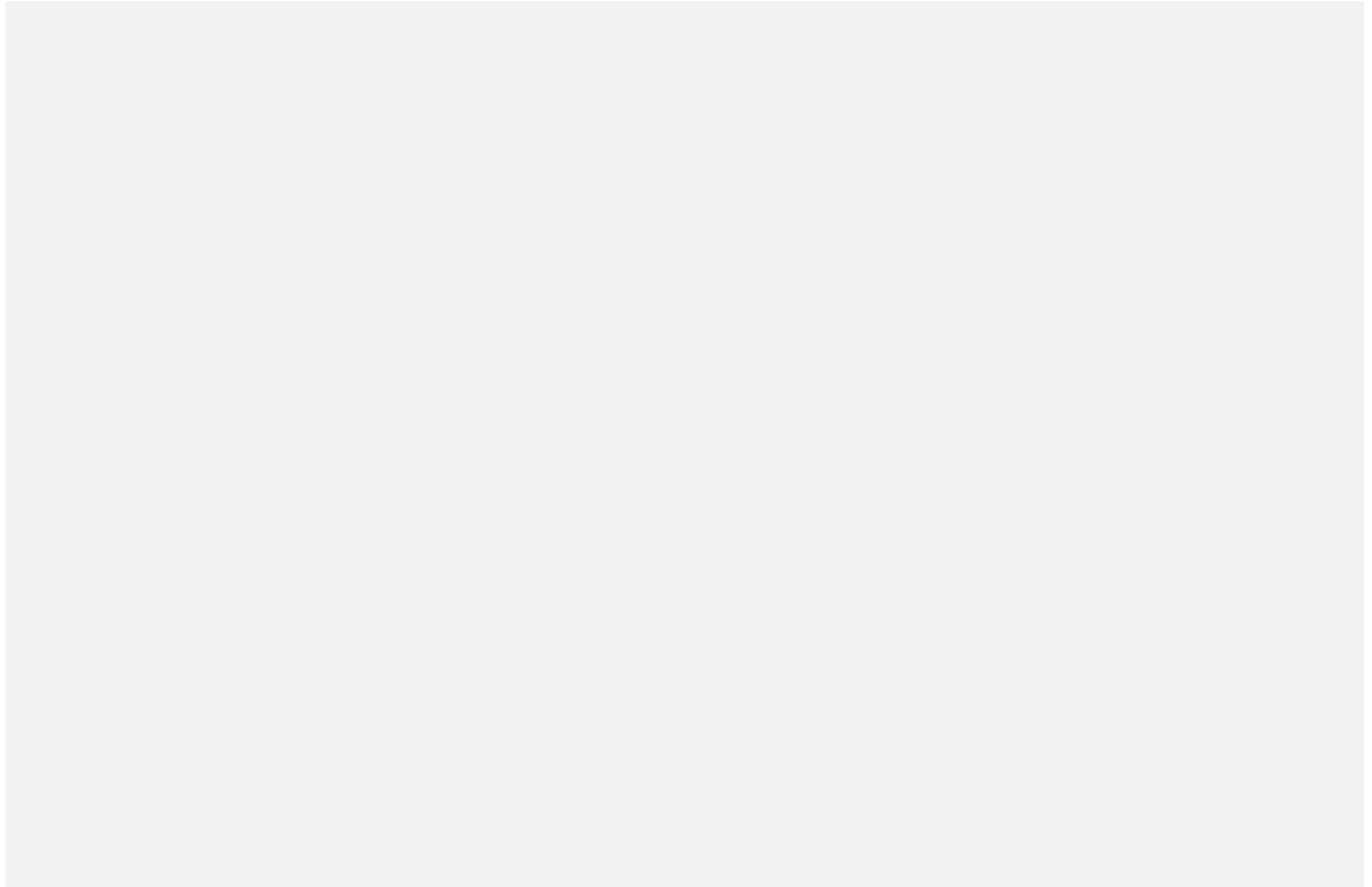
[All websites using Cloudflare receive HTTPS for free](#) using a shared certificate (the technical term for this is a multi-domain SSL certificate). Setting up a free account will guarantee a web property receives continually updated HTTPS protection. You can also explore our paid plans for individual certificates and other features. In either case, a web property receives all the benefits of using HTTPS.

## SSL Glossary of Terms

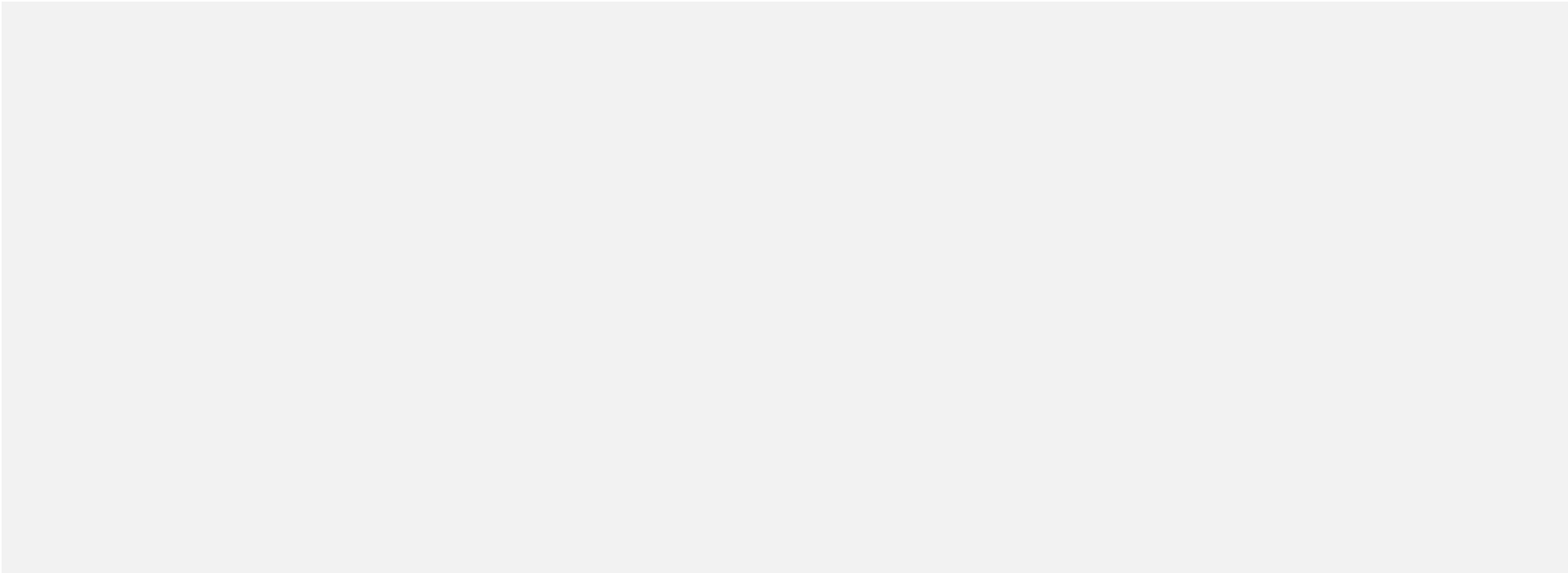












About SSL



Contact Sales:

+44 20 3514 6970

About HTTPS



About Encryption



SSL Glossary





© 2020 Cloudflare, Inc.

[Privacy Policy](#) | [Terms of Use](#) | [Trust & Safety](#) | [Trademark](#)