

Row 1

When on a HTTP site, information entered—like logins, passwords, searches, credit card numbers, emails, and so on—is visible. Governments, Internet Service Providers, and eavesdroppers can see your interactions on a site as you browse page to page.

Row 2

However, when on a HTTPS site, that information is protected by transport layer encryption. This means that the contents, and what you are looking at, are just between you and the website provider. Governments, Internet Service Providers and eavesdroppers can only see that you’re on a HTTPS website, but can’t see the specific page you are looking at.



Row 1

On HTTP sites, user information is often exposed. This includes sensitive information like logins and credit card info. On HTTPS sites, this information is protected by encryption until it arrives at the intended destination!

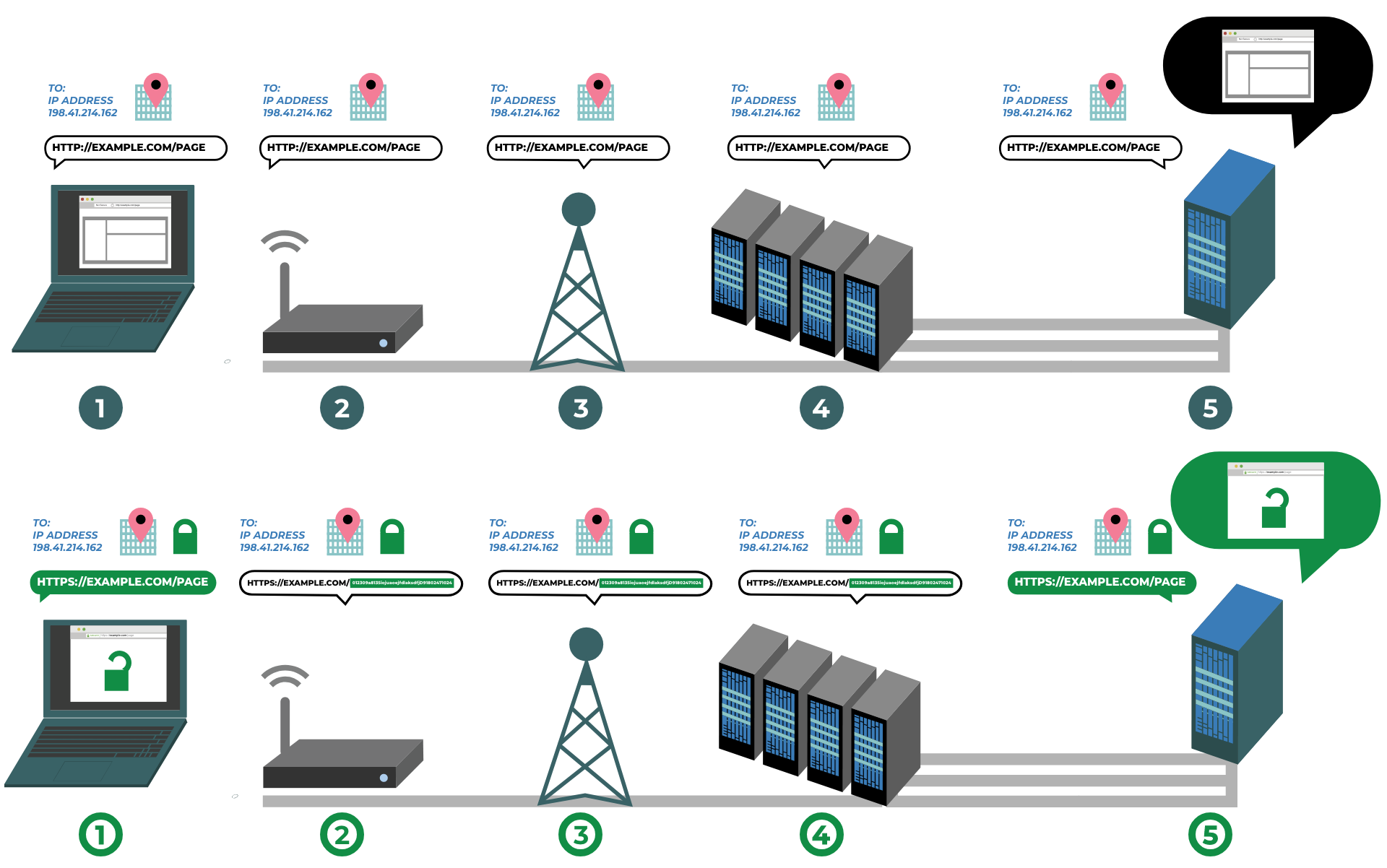
However, HTTPS is not the default for the web.

Row 2

Enter the HTTPS Everywhere browser extension!

Row 3 and 4

With the HTTPS Everywhere browser extension, HTTP requests will be upgraded to HTTPS, making your browsing more secure!



Unencrypted (top row)

Panel 1

Browsing to a web page over HTTP.

Panel 2

The router and your ISP are able to view all info sent with the request, such as login credentials.

Panel 3

Unencrypted request is sent over the network (done in "hops").

Panel 4

The unencrypted request arrives in the intended network.

Panel 5

The requested page displays what the user requested.

Encrypted (bottom row)

Panel 1

User requests page but all sensitive info is encrypted.

Panel 2

ISP and Router is aware of the site that has been requested, no other info is disclosed.

Panel 3

Network hops send through the encrypted request.

Panel 4

Encrypted request arrives in intended network.

Panel 5

Requested info is now "unlocked" (decrypted) and displayed only on successful arrival.