What Does the Website Padlock Symbol in My Web Browser Mean?

What is the Browser Padlock Icon?

Seeing the padlock icon next to a website's address gives many people a sense of security—but it's important to understand what that lock actually means.

The lock symbol simply indicates that the connection between your browser and the website is encrypted using HTTPS. This helps prevent others (like hackers on public Wi-Fi) from intercepting data as it travels between you and the website. It *does not* mean:

- The website is trustworthy
- The business is legitimate
- The content is safe or free of malware

In fact, scammers and phishing sites also use HTTPS and get SSL certificates because they're free and easy to obtain. So while the lock icon is a *good thing*, it's not a seal of approval. Always combine it with other trust signals—like a verified business name, good reviews, and your gut instinct—before entering sensitive information.

If you see that a website has a lock beside it in the search/address bar, that symbol does **not** mean you're locked out of it, **it means the website is using security** where information between your browser and the server is encrypted. It's a good thing because people between those two points cannot intercept the communication.

Websites with no security will not have this lock symbol showing.

Bottom line… websites with the padlock are good to go to. It means they're secure.

If you want to learn more about this, I've written quite a bit about this topic below and some of it gets technical. Read on…

Are Locked Websites Safe to Go To?

Yes, it means websites with a padlock in the address (or search bar) are using SSL, which is encryption between the server and your browser. The lock symbol in website address does not mean, however, that these websites are free from viruses or malware.

The website security padlock symbol in the address bar says that information between your web browser and the server is encrypted so that other people (like hackers sitting in between your browser and the web server) **cannot snoop** on what information is being sent back and forth. It looks like gibberish to them.

This is useful for when you are putting sensitive information into a website like your credit card number or social security number. Any page that you're putting that kind of information into should have that lock symbol showing so that you know the page is secure.

So don't worry – there's nothing wrong with your browser and **you didn't do anything wrong**. Like I said, it's a good thing. It's added security. Google is encouraging website owners to make all pages of their website secure, so you're going to start seeing this symbol more and more.

You do NOT want to see this – it means the information sent between your computer and the server is not encrypted:

FAQs About the Lock Symbol and Website Security

Q: Does the lock icon mean a website is safe to use?
A: Not necessarily. It only means the connection is encrypted. A secure scam site is still a scam site.

Q: Why does my browser say “Not Secure” next to a website?
A: The site either doesn’t use HTTPS, or its SSL/TLS certificate has expired or is misconfigured. You should avoid entering personal info on these sites.

Q: How do I know what kind of SSL certificate a site has?
A: Most browsers don’t show this by default anymore. You can view the certificate details by clicking the lock icon and viewing “Connection” or “Certificate.”

Q: Can I get an SSL certificate for my own site?
A: Yes. Free options like Let’s Encrypt make it easy. Many web hosts also provide one-click SSL installation.

Q: Why did Chrome replace the lock icon?
A: Starting in 2023, Chrome began phasing out the padlock because people misunderstood its meaning. It’s now a “tune” icon, which links to site permissions and settings.

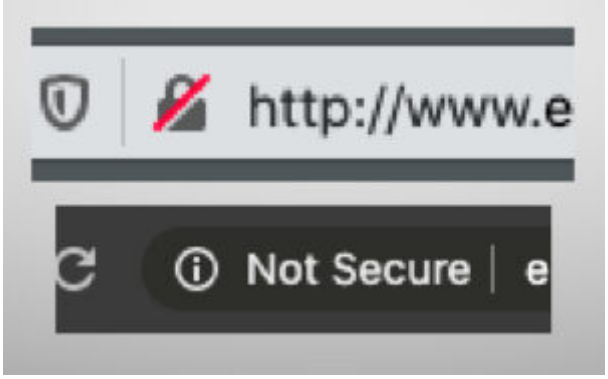
Why do Online Banking and Shopping Websites Have a Padlock Symbol?

That padlock means that the communication between your computer and them is locked. It’s encrypted so that nobody else can read what’s going on. It’s a closed/private session.

To explain how it technically works would be long and boring but here’s a basic explanation. The Internet is a public space – everyone is using it at once. You don’t have a plug in your computer that goes directly to your bank – you have a plug/connection with your computer that goes to everything. The connection is shared – that’s the Internet. It’s like a “party line” in the old days (if anyone still remembers that – I’m actually too young but I heard about it).

To get around everyone being able to snoop on your account password or how much money you have in your account (or social security numbers, credit card numbers – any private information), mathematicians and scientists came out with a way to make your connection with your bank look like gibberish to everyone else except you and your bank. It's pretty genius, actually.

Is a Website Secure if There's No Padlock Symbol?



If the Padlock is Open in the Address Bar, is it Safe?

A website with an open padlock symbol *is* safe only if you are **not** sending sensitive information to a website – like credit card info, your social security number, etc.

If there is no padlock symbol showing, then you may see a page icon or an icon with an "i" in it. This means the page was not sent to you securely. This may be just fine if there isn't any sensitive information on the page. If it's credit card page or a page sent with your contact information, then this isn't good. You should contact the website's owner and file a complaint with them.

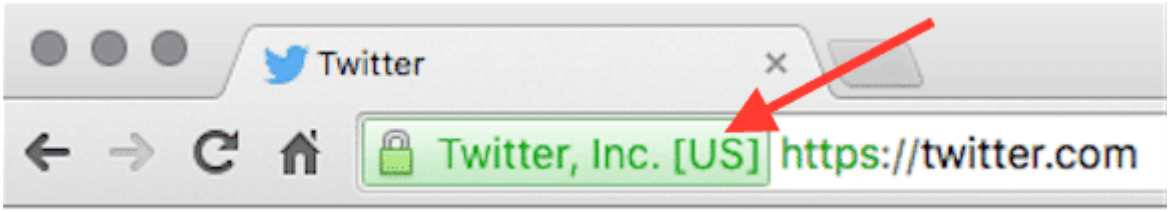
Pages that don't display a lock symbol in the web browser but have a "not secure" note or a line through the padlock means parts of the page could still be secure but that's not the best practice in website design.

You might see a message like: "The site uses SSL, but Google Chrome has detected insecure content on the page. Be careful if you're entering sensitive information on this page. Insecure content can provide a loophole for someone to change the look of the page."

It means the connection for the page itself is secure but there are one or more elements on the page that did not get transmitted securely.

It’s very easy for this to happen to a website, so don’t sweat it. One, small change to a website can trigger this. Security is still working but again, one or more elements (images, JavaScripts, etc.) are not being transmitted securely. If one image on a page isn’t secure, your credit card information is still being securely sent, so it’s fine.

An Extended Verification Certificate is Showing (VERY GOOD)



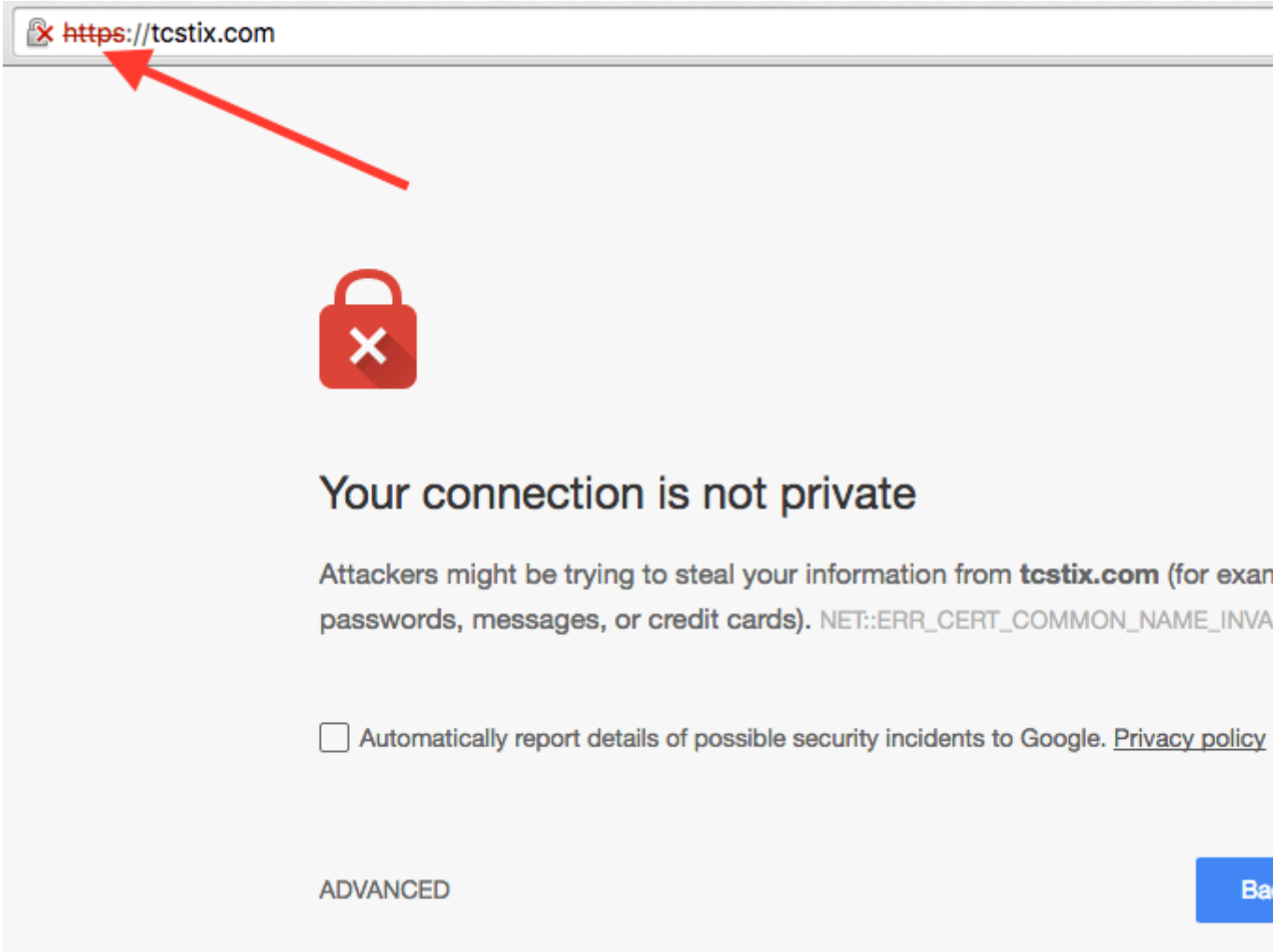
If a website has an Extended Verification Certificate, you’ll see an even bigger green bar. This kind of certificate costs more and it says that the company’s identity has been verified. Some people might even call this a “secure payment symbol.”

This extra verification means a company has been verified to be a real business. It doesn’t mean that companies without this are not real businesses but just that companies that use extended verification certificates really want to show that they are trustworthy.

Do You See https But No Padlock?

Why no padlock?

If there’s not a padlock showing on an secure website or it’s crossed out or has an “x” on it, then it might look like this:



If a website says https in the address bar but there's no padlock (and you may see a slash through it), then that could mean the website is using a secure port but there isn't an SSL certificate installed or it's not currently up to date (was not renewed).

This could show up as a "privacy error" and your web browser will display a warning before it lets you continue on to the website. It's doing this so that you know there's a page that's trying to be secure but it's not actually secure or their certificate has expired.

"This Website is Using an Invalid Certificate"

When you see this message, it means that the certificate being used isn't set up right or something doesn't match up correctly and like it should. This could simply be a web server that's not set up the right way or it could mean something else is going on. It's best to stay away from a website where this message is showing.

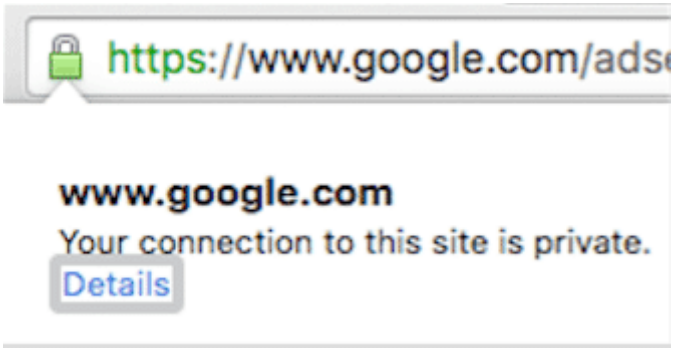
Certificate is Expired

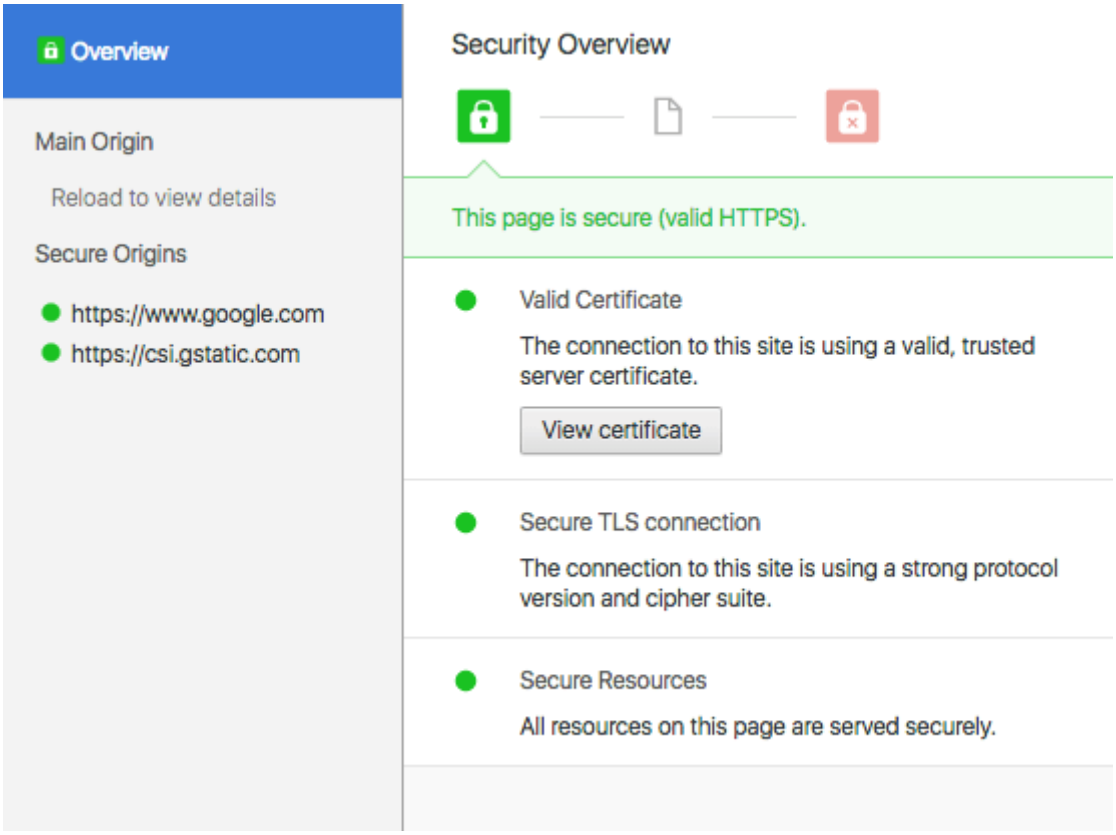
If a certificate is expired, then security is still working but the website owner or website host did not renew the security (SSL) certificate. You'll see a warning message about this but you can accept it and get past it and go to the website if you want. They DO have security set up, it's just expired. They might be working on getting it renewed.

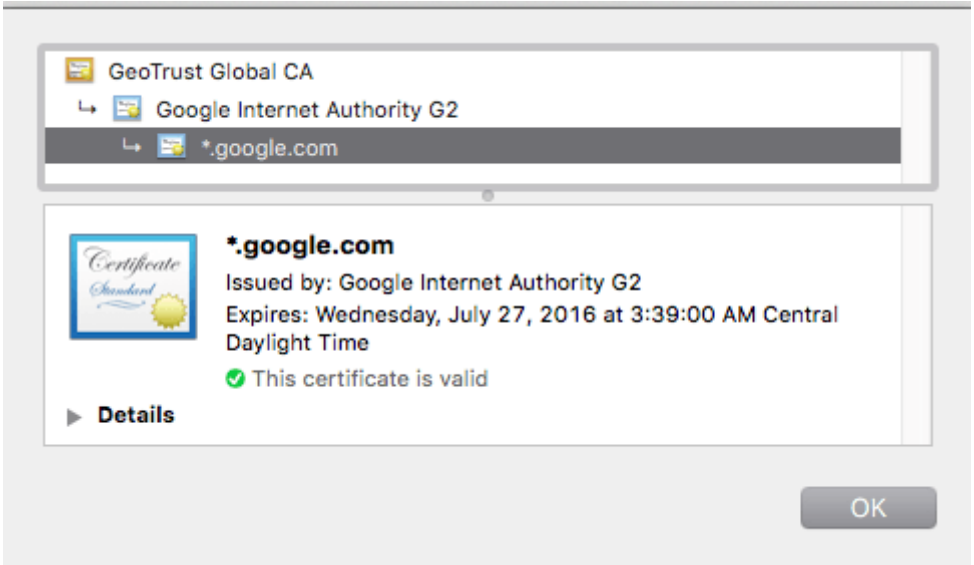
Find Out More About the Security of a Website

To learn more about how a website's security works, you can click on that lock symbol.

Click on the "Details" link and keep clicking – you can find out quite a bit:







All the lock symbol does is say if the *connection* is secure or not. You don't ever know if the website is safe (the software it uses – and no software is 100% secure) from the lock symbol – again, it's the *connection* that the lock is there for.

Still Confused?

Here's a video explaining about the secure connection in your web browser:

Look for the "https" in Your Browser's Address Bar

See if it shows "https" instead of just "http" – make sure the "s" is in the address bar in your web browser. You should see it and you may see more information about the security as well – depending on how strong the SSL is.

Basic SSL (2048 bit) is secure enough right now.

Some browsers now have the "http://" and "https://" part of the address hidden. You can turn that on if you want and I would suggest doing that so that you can better see which

pages are secure and which ones are not.

If you want to turn the http part back on in your browser bar, then here are articles on how to do it:

- Firefox: How do I get firefox to show the http:// in a web address? (support.mozilla.org)
- Safari: How to Show the Full Website URL in Safari for OS X Yosemite & El Capitan (osxdaily.com)

For Chrome, this page explains it:

How to restore the URL in Google Chrome's omnibox, i.e. always show it without right-click "Show Url" (superuser.com)

-In the omnibox, browse to chrome://flags/#origin-chip-in-omnibox
-Change the setting to "Disabled"
-If the changes don't take effect immediately (i.e. the full URL is still not shown), close and reopen Chrome

Why no Padlock? What if There Isn't a Lock Symbol on a Credit Card Page?

The problem that is most likely encountered when a page with a credit card form on it does not have the lock symbol is that there is an element or two on the page that was not transmitted to the website visitor securely.

This item can be anything from a JavaScript file to a CSS file (style sheet) to an image or video. Websites will often have a widget or code they get from another website to post on their website template and since that code has references that are http and not https, those elements end up on https page, casing the web browser to not show the lock symbol **since not every element on the page has been transmitted securely**.

What if The Lock Symbol is Broken?

Here is what you should do:

- If you notice the absence of a lock symbol on a page and you ended up on here, looking for answers, then please **contact the owner of that particular website** and make sure they know that their secure pages are missing the lock symbol. Again, those pages should show "https" and not "http" in the address bar (some web browsers are not showing the "http" part anymore, we know. There are ways of turning that back on.

- If you want a page that is not showing a lock symbol on **your website** fixed, then please contact the Website Maintenance Department at Webstix, submit a ticket and they can get you a quote on that work.

Why is There a Lock on my website?

The padlock doesn't mean the website is locked down or anything like that, it just means the page is secure and that's a good thing.

If it's on a website you own, then that's fine. It's telling people that your website is secure and they should trust it more.

How to Fix a Broken Lock Symbol if You Own the Website

To fix it, a few things can be done (by your website developer):

- Items that are not secure must be removed from pages that are secure – meaning pages that have https in the address bar.
- Write some logic into the template/theme file to not show some particular code on a page if the page is secure.
- Change (force) the URLs to https but if the domain hosting that code does not have an SSL certificate installed, then it cannot be done.

Is the SSL Certificate Expired?

Another thing that can wrong is that the SSL certificate is expired. If that's the case, then the website visitor will see a warning stating that the transaction might not be secure.

Website owners should make sure they know when their SSL certificate is set to expire so that it can be renewed before it expires – this way, people will not see this message.

The First Page Doesn't "Technically" Need to be Secure

What many people may not understand is that the page you're putting your credit card information into does **not** need to be secure itself.

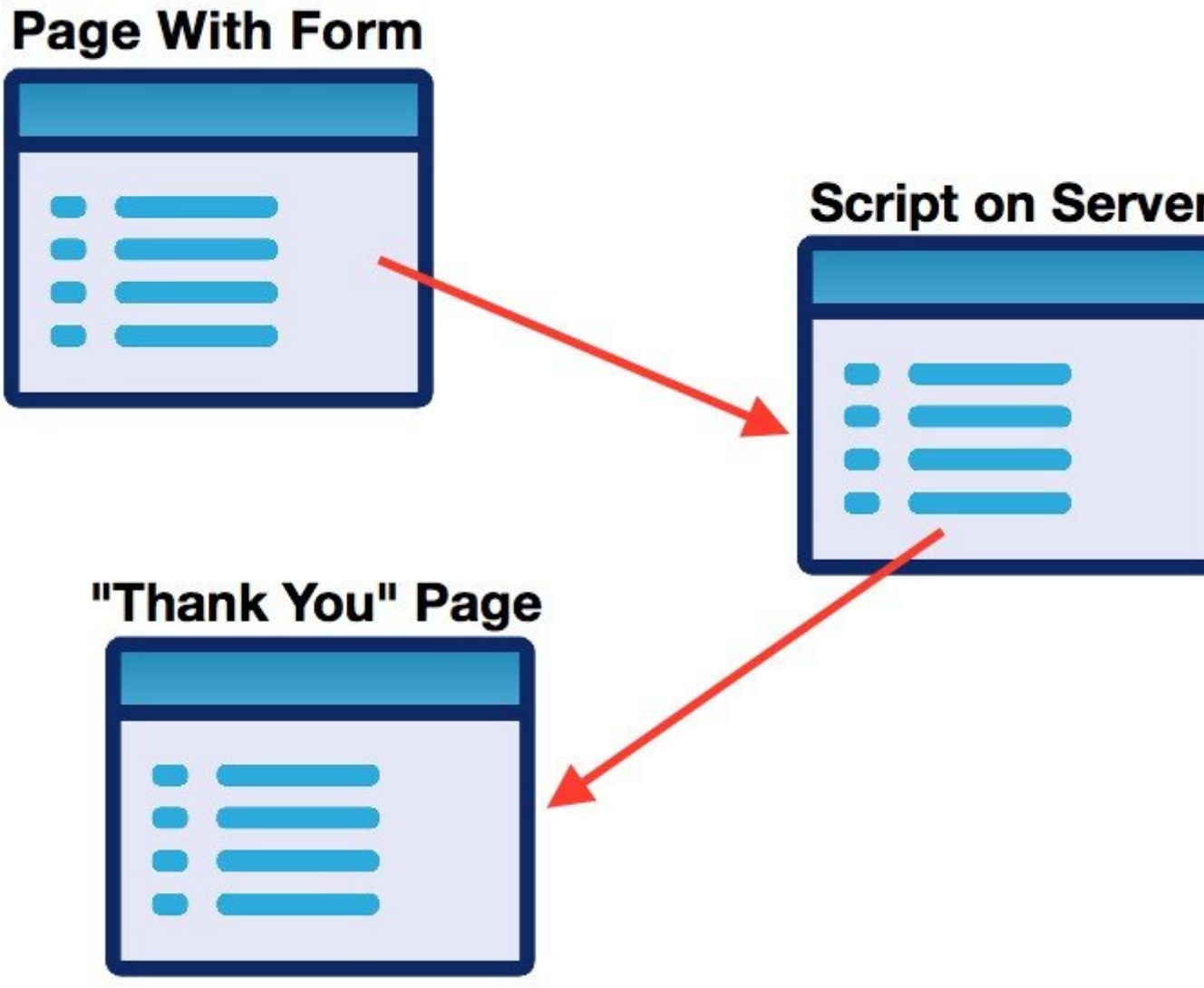
It's just a form on a page that where you put your information into. For you to first get that page containing that form, the connection did not need to be secure.

However, the page that the information is being **submitted TO** *does* have to be https for the transaction to be transmitted securely to the server.

Let's take a step back for a moment…

Forms (like credit card forms on a page) have three parts:

1. The page the form is sitting on.
2. The script (and page) the form submits to.
3. The results page – often called a "Thank You" page which indicates success.



We call the submit (clicking the "check out" button or whatever) a "post" in web lingo – the form posts to a script (computer program) sitting on your website. This is a PHP or CGI or DotNet program that does something with the information it's receiving. When you post the form to that script, that communication **does** need to be secure. That is what makes a transaction secure – well, part of it.

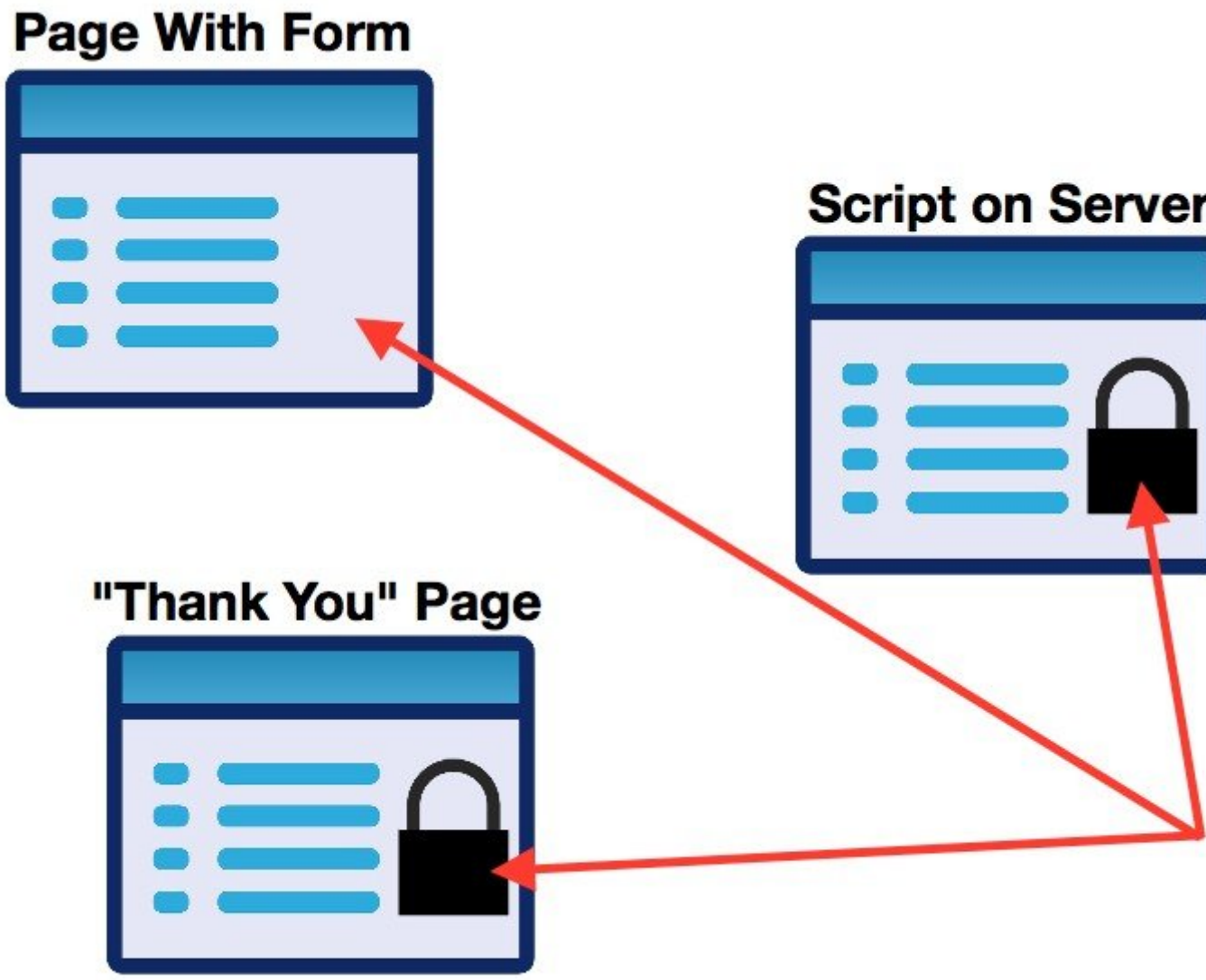
The next part of the secure transaction happens within the script itself. That script can either store the information (which it really shouldn't if it's sensitive information like a credit card or social security number) or else it does something else with it like send it through a payment gateway and subsequently from there, the payment gateway connects with a bank to see if funds are available, for example.

The communication from the script (server) to the payment gateway also needs to be secure. There's no way to tell in your web browser if that communication is secure since it's beyond your web browser – another layer deep. You just have to trust that things are set up right and that's where there's such a thing as PCI Compliance.

Does the first page need to be secure?

Technically, no. That's what I'm trying to explain here.

Here's how that is diagrammed:



This shows that the first page does not need a lock symbol (technically) but the other pages definitely do need to be secure.

Best Practices

With that said, people ARE used to seeing the lock symbol on the page that they are putting their information into. So the first page should have a lock symbol and be secure.

If that is done, then you, as the website owner, are showing your customers that you value their security and sensitive information and are conveying to them that you have adequate security in place. Having a lock in the address bar is the best practice and should be followed.

Conclusion

I hope this clears things up a bit – even though I threw a lot of information at you.

What most websites are doing now is just securing every page. That is what Google likes, so it's good for SEO. When you do this, you want to set up your .htaccess file to force SSL and make sure every page and every item on every page is secure.

If you are putting your credit card information or other sensitive information (social security number, etc.) into a website, it's best to just make sure that the page you're putting that into HAS the lock symbol in it. When you see the lock symbol on that page, you see that the website owner cares about security even though that page technically doesn't need to be secure.

If the lock symbol is not there, then your information could be sent "in the clear" which means anyone between you and the server can intercept that information and use it how they please. Protect your identity and don't become a victim of identity theft and check for that lock symbol all the time.

Oh, and if you're still using Internet Explorer for your web browser… then stop – immediately! Your computer may already be hacked. It's a really bad browser.

Stop Using Internet Explorer… Like, Now! (tonyherman.com)

Please Share!

If you found this article, please share it on Facebook, Twitter or anywhere else. Thanks!

Original article: https://www.tonyherman.com/website-secure-lock-symbol/

Special Offer for Readers

1,300+ Channels • Unlimited On-Demand Movies • **5 Devices**

$69.99/mo

Start Your Trial

Tip: Get 3 friends of family to sign up and you get streaming TV and movies for free.