



Securing your Website (SSL and Certificates)

2017 - Fall Edition

User Guide - Table of Contents

[Overview](#)

[Use Case\(s\)](#)

[SSL Protection](#)

[What will an SSL Certificate Provide?](#)

[Secured by SSL vs. Not Secured by SSL: A Quick Indicator](#)

[Browser Security Changes - Warnings](#)

[Common Questions and Concerns](#)

Overview

Website security is gaining significantly more attention as Google and other browsers have begun forcing SSL adoption. This guide covers the basics of SSL and the impact SSL Certificates (or lack thereof) have on the Member/Visitor experience on your Club's Website.

SSL stands for **Secure Socket Layer**, which is the defacto method used to encrypt sensitive data such as usernames, passwords, and other private information that is passed back and forth over the Internet between your website, visitors' browser(s), and your club's website server. An SSL Certificate provides visible assurance to visitors of the site, that the site is legitimate, and that data encryption is taking place to ensure their sensitive data is protected. Once the site has SSL, an "s" is placed after the http:// of the website's address - i.e. <https://www.anyclub.com>.

Please Note: [This short video provides more information on an SSL Certificate.](#)

Use Case(s)

- Club Web address is <http://www.yourclub.com> (missing the "s" after the http)
- Club Members are calling the Club indicating they are receiving a "Connection is Not Secure" message when visiting the Club's Website.
- When entering sensitive data into your Website, Club Members are receiving messages such as "This connection is not secure. Logins entered here could be compromised."

SSL Protection

Website's that are secured with SSL will have **HTTPS** at the beginning of their domain and will have a **green padlock** in front of the domain, seen below:



[https:// www.yourclub.com](https://www.yourclub.com)

Clubessential's SSL Certificate covers **Domain Validation (DV)**, which means that the domain ownership is checked prior to issuing the certificate.

Please Note: *The Club's Account Manager can provide clarification and assistance should you have any questions.*

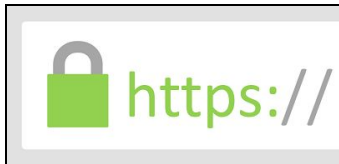
What will an SSL Certificate Provide?

Fostering a safe and secure environment for all Club activity is of the utmost importance. Passwords and credit cards are not the only types of data that should be private. Any type of data that users type into websites should not be accessible to others on the network. An SSL certificate will help **verify** the Club's Identity and will then **encrypt** any data that flows to and from the site, keeping it secure from outside users.

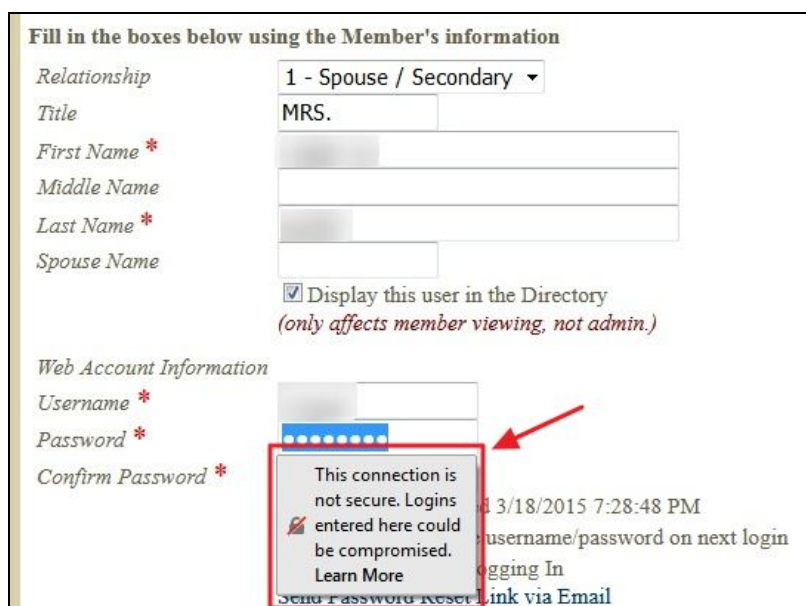
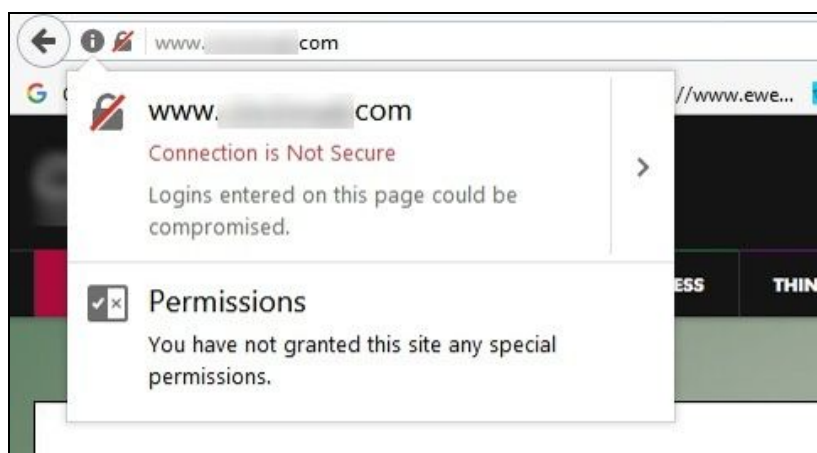
Please Note: For increased online security, most browsers are making sure users are educated on the security of the sites they visit. Find more information on this transition to a safer online environment, below.

Secured by SSL vs. Not Secured by SSL: A Quick Indicator

When you connect to a **secure** website, the URL begins with "**https**" instead of "http", like in the example below. The "s" means that the website has been secured with an SSL Certificate.



Websites **not** protected by SSL will display some type of warning in the URL bar, indicating that the "**Connection is Not Secure**", see the examples from different browsers below:

A screenshot of a web form titled 'Fill in the boxes below using the Member's information'. The form contains fields for 'Relationship' (a dropdown menu set to '1 - Spouse / Secondary'), 'Title' (with 'MRS.' entered), 'First Name', 'Middle Name', 'Last Name', and 'Spouse Name'. There is a checkbox for 'Display this user in the Directory' which is checked. Below these fields is a section for 'Web Account Information' with fields for 'Username', 'Password', and 'Confirm Password'. A red arrow points to a security warning box that appears over the password field. The warning text reads: 'This connection is not secure. Logins entered here could be compromised. Learn More'. The background of the form is light yellow.

Browser Security Changes - Warnings

Anyone using Firefox version 52 and up will see warning messages regarding their site security when they enter their password into the login field or the "Password" field in the member profiles as seen above.

Similarly, Google Chrome announced that beginning in October 2017, anyone using Google Chrome version 62 and up to view a website that's not protected by SSL, will also begin seeing "Not Secure" warning messages when entering sensitive information into online fields like password or credit card fields, or email address fields on prospective member inquiry forms. For more information from Google on this change, please see article [here](#).

Common Questions and Concerns

Q: How can I tell if a website is secured with SSL?

Websites that are secured with SSL will have **HTTPS** at the beginning of their domain and will have a green padlock in front of the domain.

Q: What kind of SSL Certificate does Clubessential use?

A: Our SSL Certificate covers **Domain Validation (DV)**, which means that the domain ownership is checked prior to issuing the certificate.

Q: Can't we just purchase our own SSL Certificate?

A: There's no need to; we'll purchase it for you and will renew it every two years. Even if you did purchase your own certificate, there's still back and forth work needed between your club and Clubessential to set up and maintain the SSL, so there will still be a fee you'll have to pay us.

Q: Does this mean our website currently is not secure because it doesn't have SSL?

A: All of your sensitive member data on the private website, behind the login screen, is already protected.

SSL is related to the Internet connection between the user and the website's server.

These days, Google wants all websites to adhere to a more secure connection using SSL (i.e., [HTTPS://www.yourwebsite.com](https://www.yourwebsite.com)) to prevent an eavesdropper from intercepting login credentials or any other sensitive information entered into data-input fields on forms.

Your members are already used to seeing HTTPS in the domains for their banks' websites. Adding SSL to your website will prevent the not secure message from appearing, thus offering reassurance to your members that your website is secure.

Q: I've seen some free SSL Certificates. Why would I pay Clubessential for SSL?

A: Most of the free SSL Certificates are actually free 90 day trials which put the onus on you to renew every 60 days or so. If you forget to renew, then your website loses its SSL. (We purchase for 2 years, and then we auto-renew the SSL certificates for you so you don't have to worry about

forgetting to do so.) Also, many web hosts that offer “free” SSL are actually bundling it with their other products and services, which you’ll still have to pay for.

Q: Why wasn’t my website secured with SSL to begin with?

A: Securing your website with SSL has not always been as pressing of a matter as it is right now.

To be frank, Google is forcing our hand.

[Google announced](#) that beginning in October 2017, anyone using Google Chrome version 62 to view a website that's not protected by SSL, will also begin seeing "Not Secure" warning messages when entering sensitive information into online fields like password or credit card fields, or email fields on forms.

Imagine if your members enter their passwords on the login screen of your website and receive the following message, “**This site is NOT SECURE.**” They're going to be concerned, and they're going to call you to see if the website is secure.

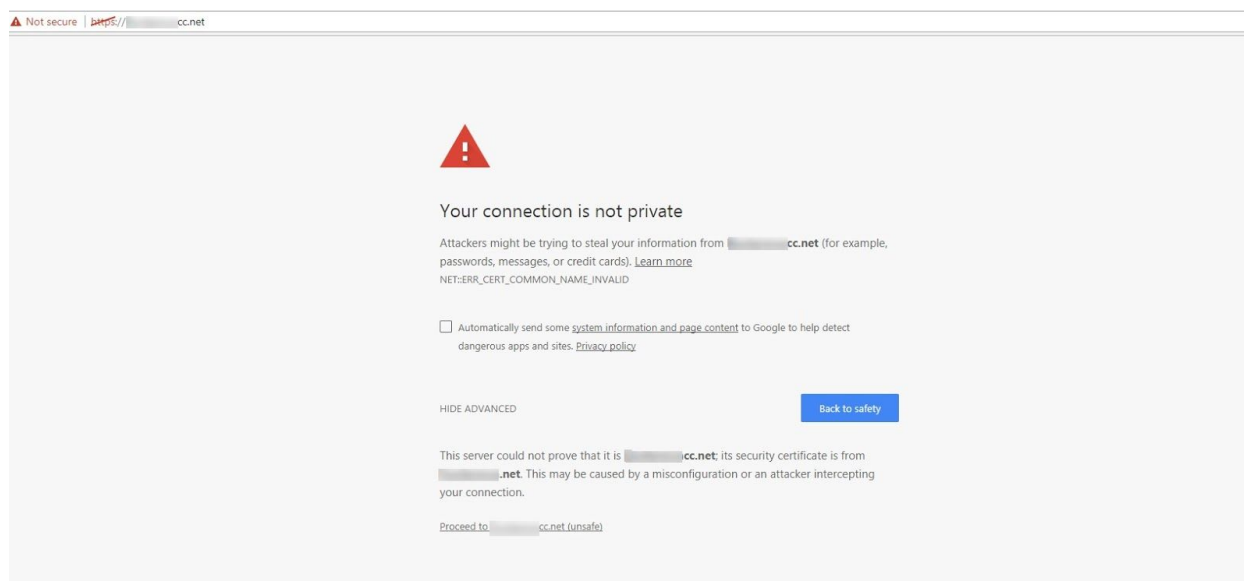
Furthermore, let’s say a potential member fills out a membership interest form on your public website... she’ll likely get the not secure warning too. That will lower your conversions and scare off some potential members.

Q: We secured our main website domain of [www.site.com](#) with SSL. We also own the domain [www.site.org](#) which redirects to [www.site.com](#). Do we need to secure [www.site.org](#) too?

A: Yes, you need to secure your redirect domains or else users will be presented with a warning / error page.

The screenshot below illustrates the following example: The website visitor is using Chrome. He enters a domain (which we've blurred to protect the client's identity) in the browser bar and hits Enter to go to that website.

The domain he entered is actually a redirect domain that goes to the main website, which has a different domain. The main website is secured by SSL, but the redirect domain is not.



According to [this Comodo article](#), this warning message is due to a Name Mismatch Error.

Name Mismatch Error

One very common error message that will show up as an SSL certificate domain name issue is a name mismatch error. There are several different possible error messages that come up based on the type of web browser used as well as the version. Some are much more ominous than others and direct the user to leave the site. Others, such as Firefox and Safari point out just what is wrong, but to the general public, the "danger" warning is really all that matters.

As if that wasn't enough, the message then recommends the viewer close the page and leave, which is certainly not what any ecommerce site wants their customers to do. Most customers assume this means a phishing site, even though it can be a simple issue with the way they actually entered the website address.

The issue that most often triggers the name mismatch error is the common name listed on the SSL certificate is not the same as the name that is typed into the address bar on the website. This means that the common name listed on the certificate might need to include the www, if it was typed in, or the web address without the www for the site has to forward to the www site for the SSL certificate.

Q: Have you ever been hacked?

A: No hacker has ever gained access to the Clubessential servers.

Q: What do you do if you suspect you are being hacked? What is your Incident Response Policy?

A: Clubessential's first response to a major attack would be to work with its security partners to immediately block the attack. Clubessential would block the intruder at the firewall if that can be done via IP address or type of protocol being used. Depending on the type of attack Clubessential might also pursue immediate legal action. Clubessential is constantly being scanned, crawled and attacked. Our email servers are attacked on a daily basis via spam.

Dictionary attacks are common and we have been through several DDoS attacks. Our firewall is strictly controlled to open only needed ports and both our firewall and Barracuda server utilize intelligent algorithms to detect and block attacks. Clubessential has also installed enough web servers to handle load spikes in the event we are attacked or have usage spikes. In the event of an attack Clubessential would immediately notify any affected clients.

Q: How often do you monitor for network intruders?

A: Clubessential's production network is constantly being monitored by Level3 and Zyedge. The internal office network is constantly being monitored by Zyedge (a company that specializes in network security and support). Clubessential also utilizes advanced security technology from Cisco, including Intrusion Detection.