How to Recognize a Secure Webpage

Just about every day there is another news story about bad things happening on the internet because someone went to a *bad* website and/or downloaded something *bad*. To be protected from being the next victim, there are a couple of guidelines to follow when accessing a website in which personal information will be provided.

First thing to know is there are two types of websites accessed on a daily basis, those that start with *http://* and those that start with *https://*. Even though it is just one letter, the 's' means a lot when you are on a website.

Below is a brief description of each:

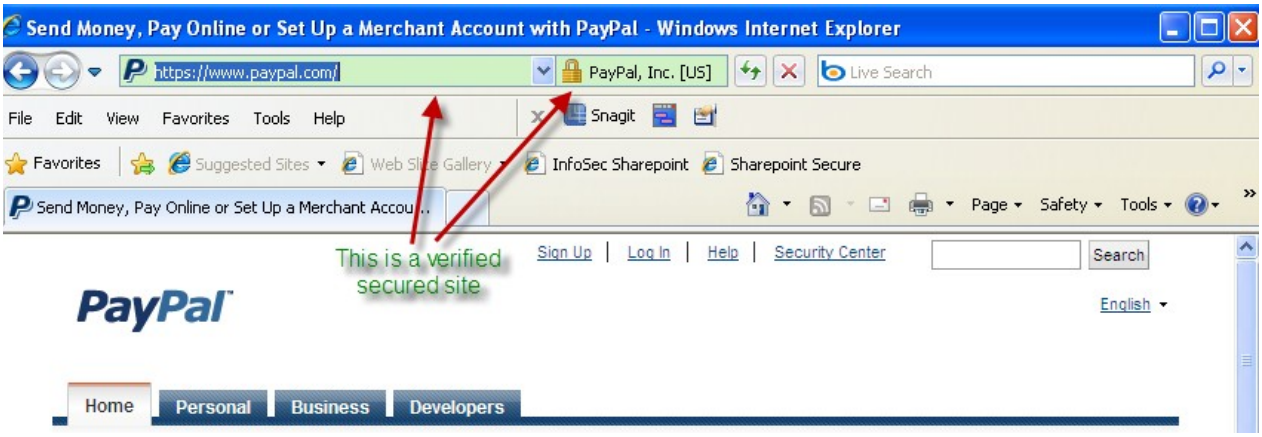
http:// -- Most websites start their address with *http://*. This is used for a website that does not require any type of encryption because there is no information being processed between you and the website. For example, if you go to http://www.amazon.com or http://www.louisville.edu, there is no reason to secure the website just to look at the website. Most likely, the user is only browsing the website and not giving away any personal information such as username and password, credit card information, etc. Once the user wants to purchase something from Amazon.com, you will see the website start with *https://*.

https:// -- This is also called SSL (Secure Socket Layer). Seeing *https://* is the first thing to look for in a website once you are asked to provide personal information. For example, once you decide to purchase an item from Amazon.com, the website changes from *http://* to *https://*. When the website changes to *https://*, your session is now being encrypted to prevent the information passed between you and the website from being compromised.

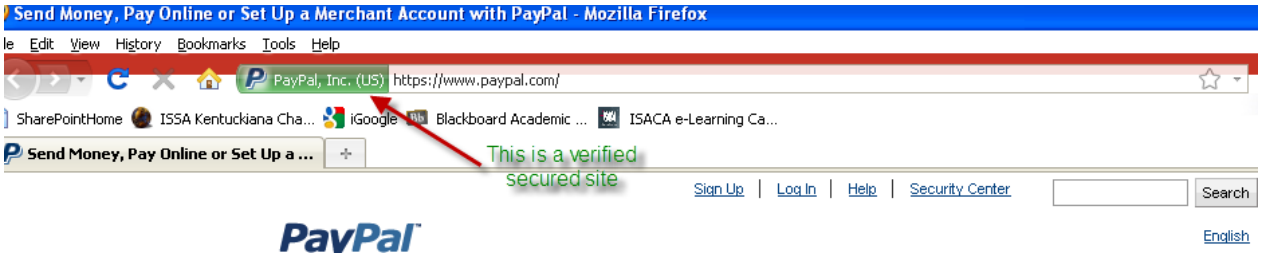
Starting a website with *https://* has been a standard for many years to protect you from malicious users attempting to eavesdrop on your information. In the past couple years, malicious users have figured out to use SSL to their advantage, so the signature authorities on the web (e.g. Verisign) have introduced Extended Validation SSL or EV- SSL. With EV-SSL, the website will still start with *https://*, but with modern internet browsers (e.g. Firefox 3.5 and above and Internet Explorer 7 and above), the user will see the address bar and/or right next to the address bar colored either green or red. *Green* means the SSL certificate is verified and *red* means it has not been verified so proceed with caution.

***Please see the next page for examples:

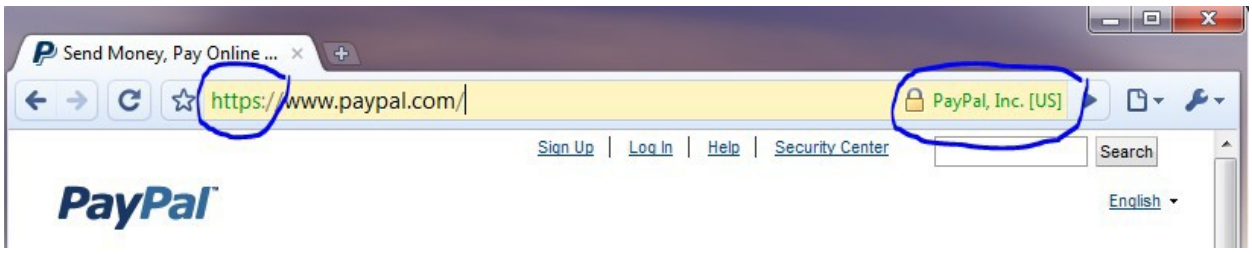
Microsoft Internet Explorer: In IE, if the secure website is verified with EV-SSL, the address bar and bar to the right of the address bar will be *green* or you will just see a lock. (You may click on the bar next to the address bar if you would like details about the verification)



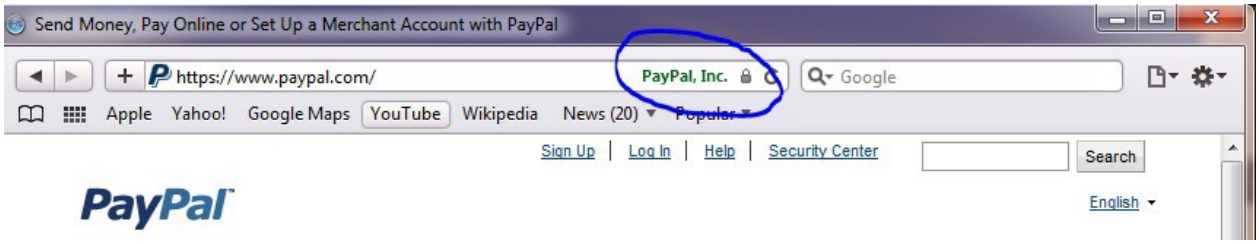
Mozilla Firefox: In Firefox, if the secure website is verified with EV-SSL, the bar to the left of the address bar will be *green* or *blue*. (You may click on the bar next to the address bar if you would like details about the verification)



Google Chrome: In Chrome, the *https:* portion of the address will be *green.* The certificate will be *green* immediately to the right of the address or you will just see a picture of a lock. (You may click on the lock next to the address bar if you would like details about the verification)



Apple Safari: In Safari, the certificate will be *green* immediately to the right of the address or there will be a picture of a lock. (You may click on the lock next to the address bar if you would like details about the verification)



What if the Bars are Red?

If the bars come up *red*, the SSL is not verified by the signature authorities on the internet (e.g. Verisign). In the case that the bar is *red*, proceed with extreme caution and do not give out any personal information.

Note: One exception to this would be if you are setting up something such as a home router. When you get into the administrative part of a router, you access it using SSL. Since this is a personal device, it will most likely not have a registered certificate unless you registered it yourself.

The moral of the story is only proceed in a SSL site if you are ABSOLUTELY sure of the source.