URL best practices

HTTPS

HTTPS (Hypertext Transfer Protocol Security) is an internet communication protocol that protects the integrity and confidentiality of data between the user's computer and site. Users expect a secure and private online experience when using a website.

HTTPS Everywhere

In October 2017, the Chrome web browser will start marking non-secure pages containing password and credit card input fields as Not Secure in the URL bar. In the future, all non-secure pages will be marked in this way.

In order to continue to improve the Weber State website, the IT Division will be switching all their core services to HTTPS only.

For the majority of Site Manager users this will have no impact.

However, power users who have references to js, css, and images using absolute links (http://www.weber.edu/MySite/some.css). Chrome will read such content as insecure and in most cases block it from even loading. This will also cause a page to show the Not Secure certificate in the search bar.

Mixed Content

Content blocked by the browser in this way is called Mixed Content.
How to avoid the Not Secure warnings in Chrome

To ensure that the Not Secure warning is not displayed on your pages you must ensure that all absolute URLs are over HTTPS (http://www.weber.edu/MySite/some.css becomes https://www.weber.edu/MySite/some.css). This includes image sources, javascript HREFs, and CSS links.