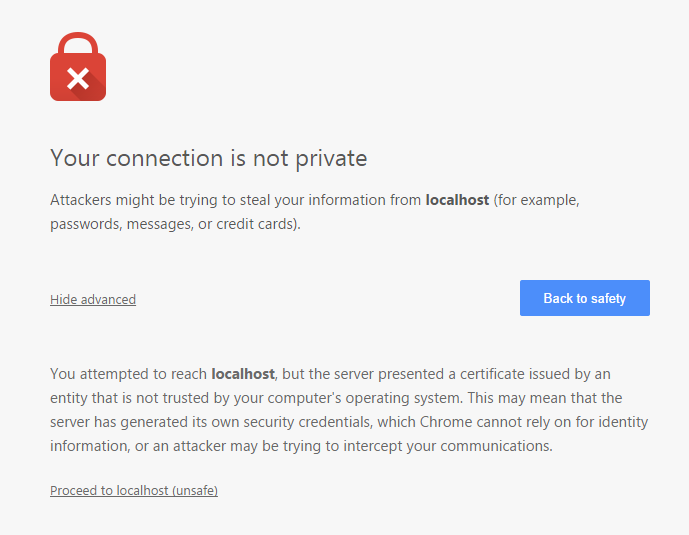
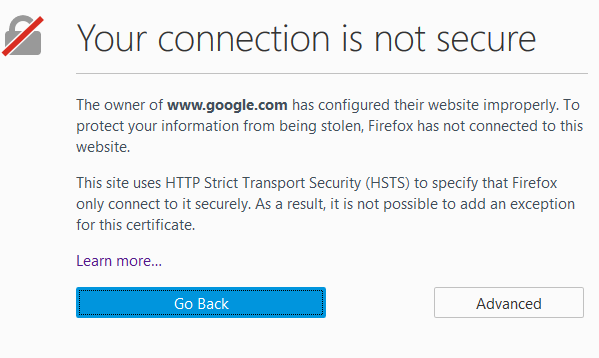
Understanding the School Email Insecurity Warning

Joseph T. Parsons

If you tried accessing Metrostate’s email or student portal anytime between about January and earlier this month, there’s a good chance you saw this big, scary warning as it appears in Google Chrome:



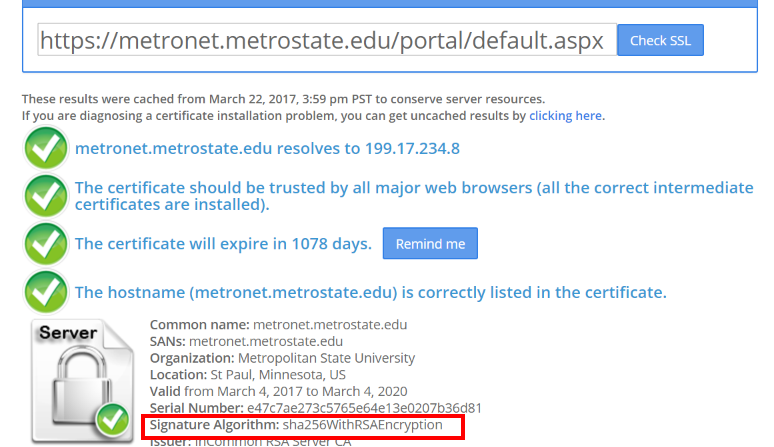
Or this equally scary warning, as it appears in Firefox:



The cause of this warning is technical, and I’d rather not bore my audience with all the nitty-gritty details. It boils down to exactly how we verify whether a site we are visiting is “real” or an “impersonation.” You see, every big site that sends or receives sensitive information (and this includes login credentials like a username and password) will try to prove that it isn’t an impersonation by first sending something akin to a “fingerprint” — something that only that site, and no one else, has.

There are a bunch of different formulas for creating this type of fingerprint, and some older formulas can be “faked.” Both Chrome and Firefox have decided very recently that one such formula, called “SHA-1,” is no longer safe enough from impersonation. So they will now warn people when visiting a site that is using SHA-1.

Metro State updated its fingerprint on March 4th to use a newer formula, “SHA-256.” If you’re still getting the warning, you may need to clear your browser cache, but most likely it will clear itself out soon enough. Additionally, you may still run across websites that haven’t updated their fingerprinting formulas, but hopefully there aren’t many remaining. In fact, most switched over to SHA-256 and other similar formulas a few years ago.



Caption: The details on Metro State’s new certificate. While the details are highly technical, the important takeaway here is the signature algorithm. It is now SHA-256, whereas before it was the older, insecure SHA-1.