COMMONWEALTH
OFFICE OF
TECHNOLOGY

COT Security Alert – Google Sunset on SHA-1 Certificates

Recently Google has announced changes in how secure sites will appear with certain types of SSL certificates in their browser, Chrome. SHA-1 and SHA-2 are cryptographic ‘hash’ algorithms used in the digital signatures making SSL certificates work to secure a site. Many secure sites using an SSL certificate (https:// indicates a secure site) currently are protected with SHA-1 hash certificates. Google’s changes will require SHA-1 hash certificates to be replaced with the more complex SHA-2 in order for end-users and the public to be able to affirm site security for business or other secure transactions. The certificate information for a site is found by clicking the lock icon in the browser’s address bar. Even if the site is protected with a SHA-1 certificate, the indicators on the site will indicate otherwise over time with these Google Chrome updates.

The schedule Google has adopted for SHA-1 certificate deprecation enforcement in their browser, Chrome, is aggressive. While Microsoft has a less aggressive schedule, it is anticipated that some other browsers may follow suit after Google Chrome. Most business owners will not want users to have a bad experience on their site regardless of the browser they use.

In addition, SSL certificates have levels of this encryption, including the chain level. SSL certificates may be SHA-2 at the business level, but at the deeper chain level remain SHA-1. This is the Google schedule and what will happen to current certificates if they are SHA-1, even at chain level, based on the certificate expiry date:

Chrome Version	**Release Date**	**Expiration before Jan 2016**	**Expiration Jan-May 2016**	**Expiration June-Dec 2016**	**Expiration after 2016**
39	11/3/2014	No change	No change	No change	Caution symbol on lock
40	12/15/2014	No change	No change	Caution symbol on lock	No lock or security (same as HTTP)
41	01/26/2015	No change	Caution symbol on lock	Caution symbol on lock	Red X and red line through https in address bar, caution symbol if chain certificate only is SHA-1

Entrust will provide SHA-2 chain certificates beginning September 30, 2014. When they do, a full SHA-2 certificate may be applied to a site and the user will know the site is protected.

The effort by technical staff to renew certificates will begin when the SHA-2 chain certificate is available. COT will ensure web applications and sites under their management are secured with SHA-2 certificates before the deadlines set by Google. We will also assist agencies who maintain their own sites to renew before the sunset. There is no charge for the new certificates.

If a server or operating system is in place that will not support SHA-2, or if SSL certificates were issued through other vendors and without COT involvement, business owners may need to plan accordingly.

Please find more information here:
http://www.entrust.com/chrome-sun-setting-sha-1/
https://casecurity.org/wp-content/uploads/2014/09/SHA-256-Support-List.pdf

NOTICE: COT is providing this information so that you are aware of the latest security threats, vulnerabilities, software patches, etc. You should consult with your network administrator or other technical resources to ensure that the appropriate actions for these alerts are followed. If you are a network administrator and need additional information, please call the Help Desk at 502.564.7576.

Office of Chief Information Security Officer
Commonwealth Office of Technology
120 Glenn's Creek Road, Jones Building
Frankfort, KY 40601
technology.ky.gov

Technology-enabled Business Solutions for 21st Century Government