Known Issue: Contacts see a privacy message after clicking email links

This article applies to:

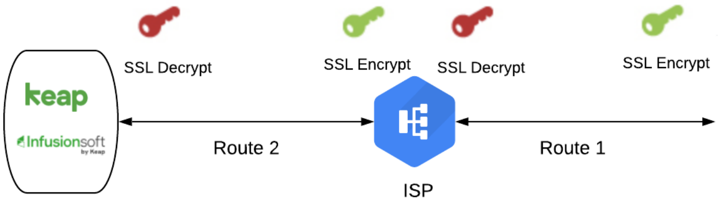
Since January 13, 2020 Keap has received reports (Known Issue 1921120) that when email recipients click a link in an email they may encounter a Google privacy/security warning page stating that the connection to the site they are attempting to access is not private or unsecure. This issue is due to recent browser updates and whether some Internet Service Providers support newer security protocols. We have confirmed that some of these affected links are now working correctly without displaying the privacy/security warning message.

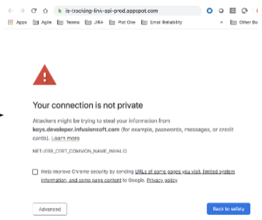
What Happened?

Google recently released version 79 of Chrome. This version ended support for older versions of a security protocol when communicating across the internet (TLS 1.0 and 1.1). Other browsers followed within a few days. You can read more here.

Many computers automatically updated to this latest version and, as a result, if any Internet Service Providers had proxy servers that did not support the newer versions of the security protocol, the privacy message would be displayed in the user’s browser.

On January 21, 2020 Google also changed it’s SSL key for their appspot.com domain to provide the secure connection between a browser and the target server. Keap’s Tracking-Link Service (which allows our reports to indicate who clicked links in your emails) uses the appspot.com domain. The SSL Key needs to be the same on the browser and server for a secure connection. If these are different, the privacy message will appear. Please note that when these keys change, it does take time to propagate the change through the internet.





Your connection is not private

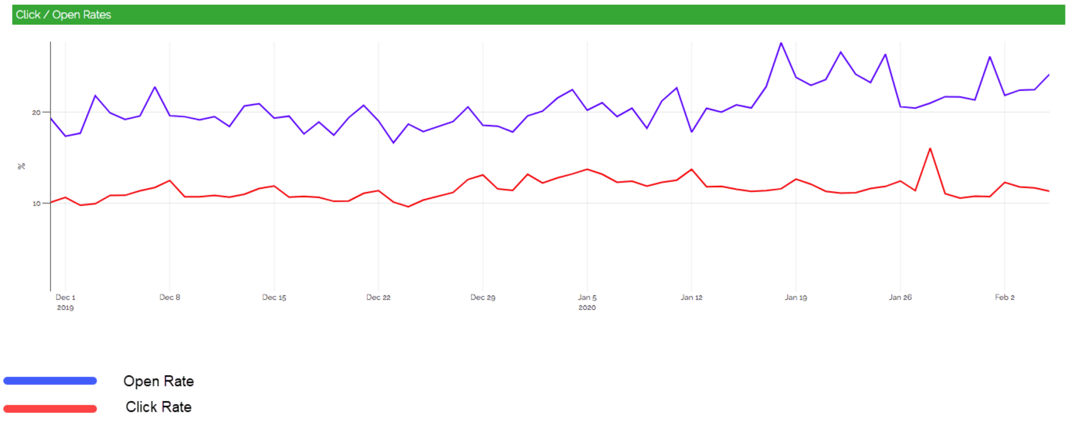
Attackers might be trying to steal your information from **keys.developer.infusionsoft.com** (for example, passwords, messages, or credit cards). Learn more

NET::ERR_CERT_COMMON_NAME_INVALID

□ Help improve Chrome security by sending URLs of some pages you visit, limited system information, and some page content to Google. Privacy policy

If either of the SSL Keys or other Transport Protocols do not match in Route 1 or Route 2 the warning page is displayed

While frustrating, this affected only a small percentage of Keap customers' email recipients. The graph below shows no negative trend, holistically, on email opens and click rates across our user base.

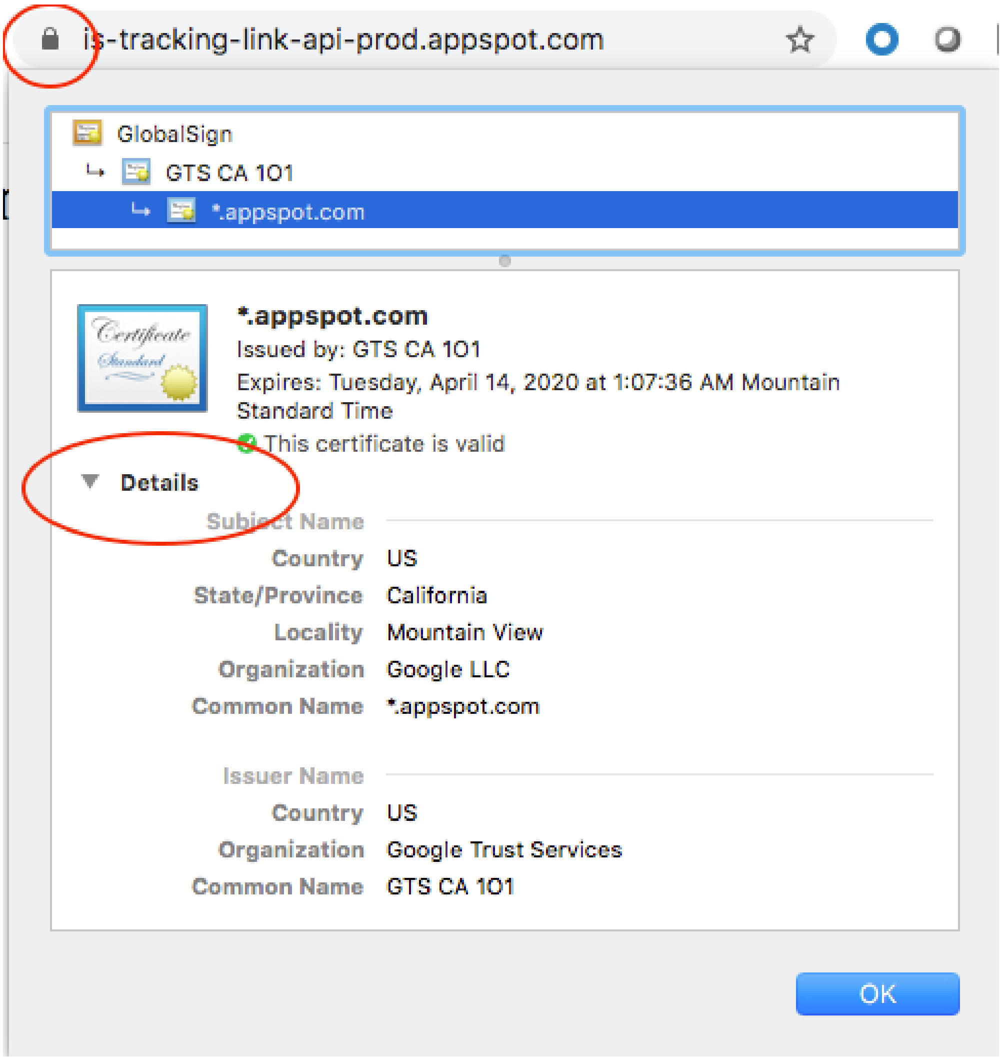


What can Keap do to prevent this in the future?

While a technical issue such as this is outside of Keap's control, we did investigate promptly and identified that thousands of applications use the Google owned appspot.com domain and therefore the reputation of this domain does get degraded. In addition, Internet Service Providers may route requests to appspot.com domains through extra security servers that may have added to this issue. Keap did use this domain to track recipients clicking links. This domain has now been switched out to a Keap owned domain where we can better control our sending reputation.

What can Keap customers do?

This issue may still exist while Internet Service Providers are updating servers. If you receive any communication from your customers on this issue, please ask them to click the lock next to the URL bar in their browser and select Certificates. Clicking ‘details’ will display the *.appspot.com certificate and the owner, which should be Google. If it is not Google, please ask for a screenshot and send it to our support group.



***.appspot.com**

Issued by: GTS CA 1O1

Expires: Tuesday, April 14, 2020 at 1:07:36 AM Mountain Standard Time

This certificate is valid

▼ Details

Subject Name	
Country	US
State/Province	California
Locality	Mountain View
Organization	Google LLC
Common Name	*.appspot.com
Issuer Name	
Country	US
Organization	Google Trust Services
Common Name	GTS CA 1O1

If the certificate is owned by Google, you can explain the issue as detailed above and tell your customer to click the Advanced link in the message and they can proceed to your site.

We understand that technical issues such as this are frustrating and security is paramount at Keap. We appreciate your patience while we continue to investigate this issue and work to ensure our systems are resilient.