Google

Transparency Report Reports About FAQ

Email encryption in transit Overview

Email encryption in transit

When an email is encrypted in transit with a security protocol called transport-layer security (TLS), it is harder for others to read what you're sending. A growing number of email providers are working to encrypt email messages in transit. The data here shows the current state of email encryption in transit.

Encrypted traffic to and from Google

Many email providers don't encrypt messages while they're in transit. When you send or receive emails with one of these providers, your messages are as open to snoopers as a postcard in the mail. A growing number of email providers are working to change that by encrypting messages sent to and from their services using Transport Layer Security (TLS). Generally speaking, use of encryption in transit continues to increase over time, as more providers enable and maintain their support. Factors such as varying volumes of email may explain other fluctuations in these encryption statistics.

WHAT IS ENCRYPTION?

Google

Transparency Report Reports About FAQ

Email encryption in transit Overview

Google

Transparency Report

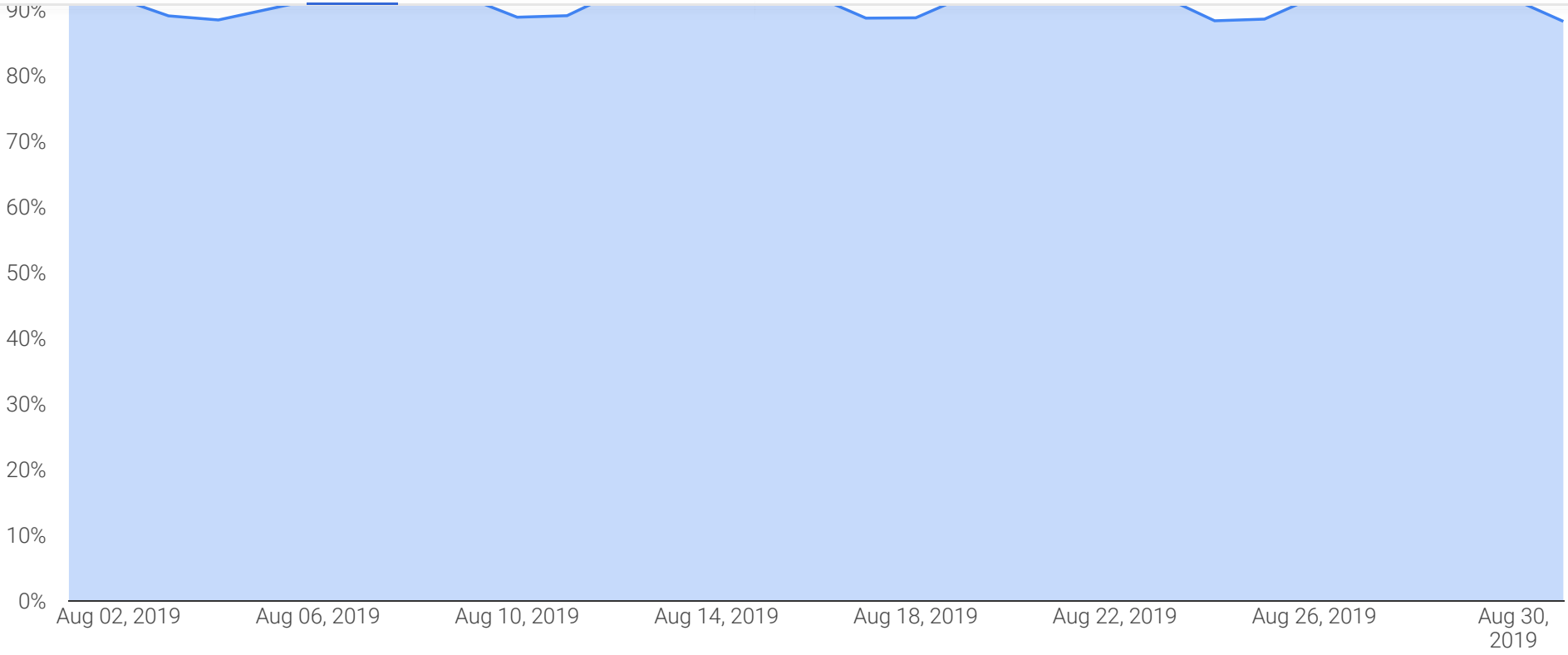
Reports

About

FAQ

Email encryption in transit

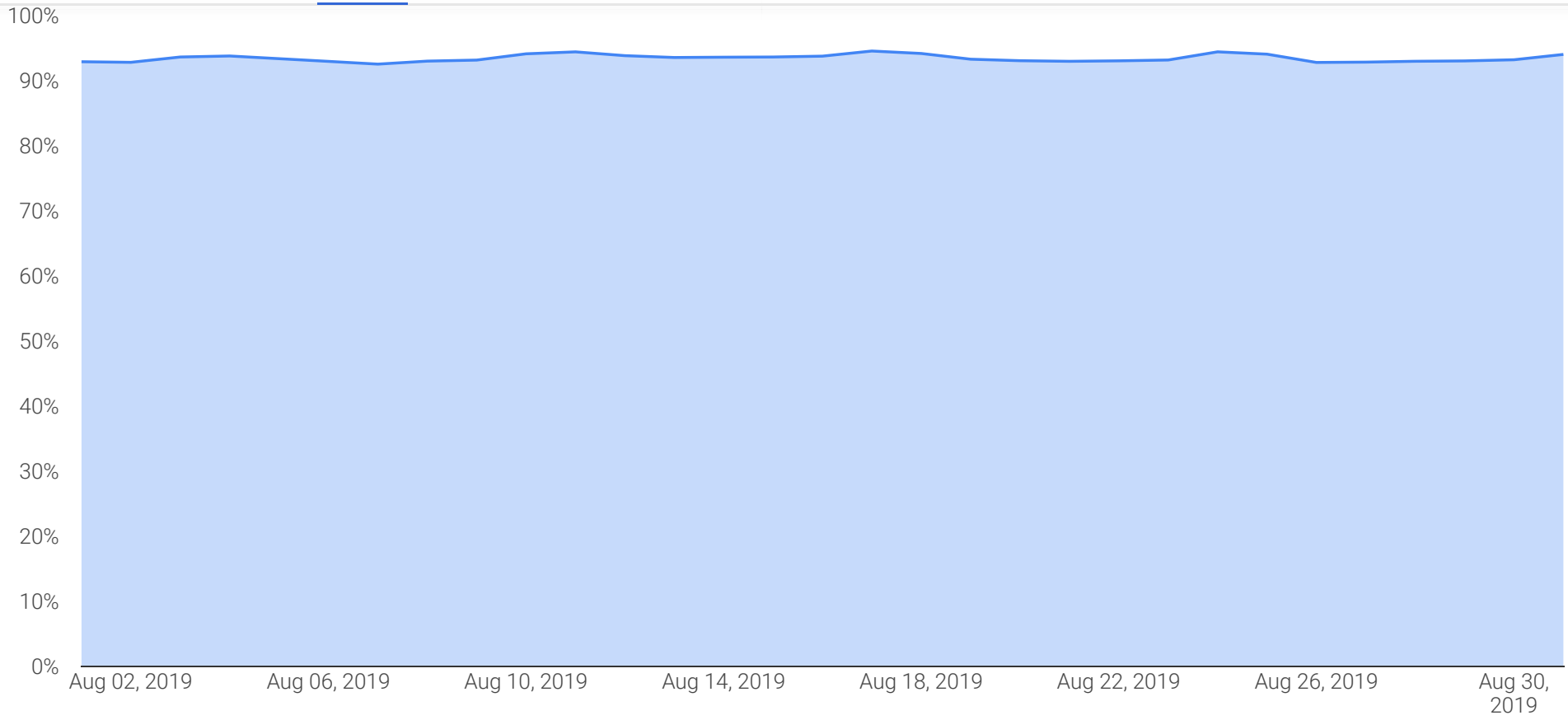
Overview



Google

Transparency Report Reports About FAQ

Email encryption in transit Overview



Google

Transparency Report Reports About FAQ

Email encryption in transit Overview

Support for encryption in transit

Below is the percentage of emails encrypted for the top domains in terms of volume of email to and from Gmail, in alphabetical order.

Select a region

World

Top domains by region: Inbound

RED YELLOW GREEN

Google

Transparency Report Reports About FAQ

Email encryption in transit Overview

From: irctc.co.in	87%
From: ofertasbmc.com.br	2%
From: secureserver.net	73%
From: timesjobs.com via tbsl.in	0%
From: wattpadmail.com	0%
From: yahoo.co.jp	0%

Sun, Sep 15, 2019

Top domains by region: Outbound

Google

Transparency Report Reports About FAQ

Email encryption in transit Overview

To: ezweb.ne.jp	0%
To: istruzione.it	9%
To: nauta.cu via etecsa.net	0%
To: softbank.jp	0%
To: softbank.ne.jp	0%
To: sympatico.ca via bell.net	0%
To: yahoo.co.jp	0%

Sun, Sep 15, 2019

How encryption works

If you mail a letter to your friend, you're hoping that she'll be the only person who reads it. But a lot could happen to that letter on its way from you to her, and there may be prying eyes who try to read it. That's why we send important messages in sealed envelopes rather than on the back of postcards. Sending and receiving email works in a similar way. But when you send or receive messages with an email provider who doesn't transmit messages via a secure connection, your emails could be open to snooping.

Google

Transparency Report Reports About FAQ

Email encryption in transit Overview

Your messages are encrypted only if you and the people with whom you you exchange email both use email providers that support Transport Layer Security. Not every email provider uses TLS, and if you send or receive messages from a provider that doesn't, your message could be read by eavesdroppers. While TLS isn't a perfect solution, if everyone uses it, snooping on email will be more difficult and costly than it is today.

Let's make email safer.

More messages encrypted in transit make emails safer for all of us.

DOWNLOAD REPORT DATA

FIND OUT HOW SECURE YOUR EMAIL PROVIDER IS

Google

Transparency Report Reports About FAQ

Email encryption in transit Overview

About

FAQ

Safe Browsing: malware and phishing

Email encryption in transit

HTTPS encryption on the web

Android ecosystem security

Government requests to remove content

Requests to delist content under European privacy law

YouTube Community Guidelines enforcement

Removals under the Network Enforcement Law

Traffic and disruptions to Google

Google Help Privacy About Google Send feedback English