

Google introduced a new email encryption application

In order to reassure their users about privacy, Google has not only released a privacy report but also launched a new full encryption tool.

In order to reassure their users about privacy, Google has not only released a privacy report but also launched a new full encryption tool.

In order to reassure their users about privacy, Google has not only released a privacy report but also launched a new full encryption tool. In the privacy report, Google launched a new section to make it clearer about its ability to protect users from eavesdropping: " *We sent important messages in sealed mailboxes, not must be greeting cards . So are e- mails . E- mails are encrypted from senders to recipients, like in envelopes, and will be less eavesdropped - regardless of crime or governments* " .

Currently, Google uses TLS encryption to send and receive email through Gmail. However, users also need to ensure that their email browser also uses TLS. According to Google, about 50% of emails are sent between Gmail and other unencrypted services.



In the chart above, Google has clarified the non-coding rate for exchange emails and other services. At the same time, the search giant also launched a new email encryption application called *End-To-End*. Users can use this application by downloading the corresponding *extension* (*extension*) on Chrome. Currently, the above extension is limited to Chrome application developers. According to Google, end users will soon be able to use the secure email encryption utility in the future.

In the privacy report, Google launched a new section to make it clearer about its ability to protect users from eavesdropping: " We sent important messages in sealed mailboxes, not must be greeting cards, so are emails, emails are encrypted from senders to recipients, like in "envelopes", and will be less eavesdropped - whether by criminals or by themselves. cover "

Currently, Google uses TLS encryption to send and receive email through Gmail. However, users also need to ensure that their email browser also uses TLS. According to Google, about 50% of emails are sent between Gmail and other unencrypted services.

Top domains by region, inbound			Top domains by region, outbound		
Domain	%		Domain	%	
From: amazon.{...} via amazonses.com	99.9%		To: aol.com	99.99%	
From: amazonses.com	99%		To: comcast.net	< 1%	
From: constantcontact.com	< 1%		To: craigslist.org	99.9%	
From: ed10.net via ed10.com	0%		To: hotmail.{...}	> 50%	
From: facebookmail.com via facebook.com	100%		To: live.{...} via hotmail.{...}	> 50%	
From:grouponmall.{...}	0%		To: mail.ru	< 50%	
From: hotmail.{...}	> 50%		To: me.com via akadns.net	0%	
From: linkedin.com	> 95%		To: msn.com via hotmail.{...}	> 50%	
From: twitter.com	99.9%		To: sbcglobal.net via yahoodns.net	100%	
From: yahoo.{...}	99%		To: yahoo.{...} via yahoodns.net	100%	

In the chart above, Google clarified the non-coding rate for exchange emails and other services. At the same time, the search giant also launched a new email encryption application called End-To-End. Developers can use this application by downloading the corresponding *extension* (*extension*) on Chrome.

Currently, the above extension is limited to Chrome application developers. According to Google, end users will soon be able to use the secure email encryption utility in the future.

You finished reading the article "**Google introduced a new email encryption application**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.