

Google toughens security with Gmail encryption (Update)

March 20 2014, by Rob Lever



A woman looks at her e-mail on a computer screen in Washington on November 23, 2010

Google said Thursday its popular Gmail service would use encryption to thwart snooping, in the latest move by the tech sector reassuring customers following revelations about US surveillance programs.

"Your email is important to you, and making sure it stays safe and

always available is important to us," Gmail engineering security chief Nicolas Lidzborski said in a blog post.

"Starting today, Gmail will always use an encrypted HTTPS connection when you check or send email.

"Today's change means that no one can listen in on your messages as they go back and forth between you and Gmail's servers—no matter if you're using public WiFi or logging in from your computer, phone or tablet."

Google has already begun scrambling most of the traffic at its websites as technology firms grapple with moves by US intelligence agencies to spy on what people are doing and sharing online.

And similar moves have been announced by Yahoo, Microsoft and Facebook to use encryption that limits the ability of a third party to read messages or emails.

US tech firms have been ramping up encryption since last year's explosive revelations about the vast surveillance capabilities of the National Security Agency and other intelligence services, based on leaked documents.

Lidzborski said Google's latest move "ensures that your messages are safe not only when they move between you and Gmail's servers, but also as they move between Google's data centers—something we made a top priority after last summer's revelations."

Some reports say the NSA had been able to access the data centers of Google and other Web firms.

Experts say encryption generally prevents outsiders from intercepting a

person's messages or documents, but that a persistent effort can gain access through malware or other methods that trick a person into revealing passwords.

NSA-proof?

Joseph Hall, chief technologist at the Center for Democracy and Technology, said Google's move is positive even if it does not protect against every potential threat.

"I'm reluctant to say anything is NSA-proof," Hall told AFP.

"But I think what Google is trying to do is make sure they come through the front door and not the back door."

Hall said that Google's encryption "would make it very difficult" for the NSA or others to tap into email traffic directly.

But he cautioned that the encryption would be only for "transport" and that data may still be unencrypted while sitting on a user's browser or stored in certain data centers.

Still, he maintained that this encryption is positive because it is "part of a general trend of strengthening the core Internet structure."

"Unfortunately, this is a case of an American Internet company having to beef up security because of attacks by its own government," Hall said, while adding that it could be positive for people living in authoritarian regimes.

"If you're an activist in Syria or and Iranian democracy activist, it will go a long way to making you secure."

Google's announcement came a day after co-founder Larry Page condemned US government snooping on the Internet as a threat to democracy.

Page, speaking at the Technology Entertainment Design (TED) gathering in Canada, was sharply critical of the NSA.

"It is tremendously disappointing that the government sort of secretly did all this stuff and didn't tell us," Page said.

© 2014 AFP

Citation: Google toughens security with Gmail encryption (Update) (2014, March 20) retrieved 13 April 2024 from <https://phys.org/news/2014-03-google-gmail-encrypted-today.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.