

17 June 2009

By: Lucian Constantin, Web News Editor

[Security and Privacy Gurus Plead to Google for Default HTTPS](#)



Google considers enforcing HTTPS by default for Gmail, Docs and Calendar Google (for the original logo)

The company considers it and commits to trial tests

Thirty seven security researchers, professionals, privacy advocates and academics have sent a letter to Google's CEO, Eric Schmidt, asking him to consider encrypting all connections to Gmail, Google Docs and Google Calendar by default. Google has openly replied that it is considering such an implementation and will start tests on small groups of users.

Hypertext Transfer Protocol Secure (HTTPS) refers to HTTP connections that benefit from a form of encryption. This protocol has been supported by all major browsers since as far back as 1994, and Google already enforces it in order to protect sensitive data passing through Google Voice, Health, AdSense and Adwords.

The technology is also available for Gmail, Google Docs and Google Calendar, but it requires users to opt in to it, either by manually adding the https:// extension to the URLs or, more recently, by enabling it as a default on the Gmail Settings page. The experts signing the letter sent to Google claim that this feature is not advertised enough, nor is it easy to locate for the average user.

Furthermore, they maintain that the performance impact of having it enabled by default for everyone is negligible, compared to the security benefits. To back up their request, they exemplify with both theoretic and real-life attack scenarios where ill-intent individuals could or did sniff the unencrypted data passing over wireless networks. Previously [demonstrated](#) man-in-the-middle account hijacking attacks based on stealing session cookies are also mentioned.

"We strongly urge you to follow the lead of the financial industry and enable HTTPS encryption by default for the users of Google Mail, Docs, and Calendar," the world-renowned security and privacy minds write to Eric Schmidt. "As Google's own help page notes, mail inboxes often contain 'sensitive data… like bank statements or online log-in credentials.' Given the huge threat posed by identity theft, it is vital that Google take proactive steps to protect its users from these risks," they conclude.

In a [post](#) on the company's Online Security Blog, Alma Whitten, software engineer within Google's Security & Privacy Teams, publicly responds to this report. "We're currently looking into whether it would make sense to turn on HTTPS as the default for all Gmail users," she announces. "[...] The additional cost of offering HTTPS isn't holding us back. But we want to more completely understand the impact on people's experience, analyze the data, and make sure there are no negative effects," she goes on to explain.

In this respect, the company plans to start trial tests on "small samples of different types of Gmail users." It is also noted that, "Unless there are negative effects on the user experience or it's otherwise impractical, we intend to turn on HTTPS by default more broadly, hopefully for all Gmail users."

On the downside, connections over HTTPS are slower, because, compared with HTTP, the data needs to also be encrypted and decrypted at both ends, resulting in bigger delays. This might be unnoticeable in countries where the broadband connection is the standard, but

might pose problems for users living in underdeveloped regions, where dial-up Internet access is still the only affordable option.