Volume of encrypted email rising amid spying fears (Update 2)

3 June 2014, by Michael Liedtke

The volume of email cloaked in encryption technology is rapidly rising as Google, Yahoo, Facebook and other major Internet companies try to shield their users' online communications from government spies and other snoops.

Google and other companies are now automatically encrypting all email, but that doesn't ensure confidentiality unless the recipients' email provider also adopts the technology.

In an analysis released Tuesday, Google Inc. said that about 65 percent of the messages sent by its Gmail users are encrypted while delivered, meaning the recipient's email provider also supports the technology. That's up from 39 percent in December. Incoming communiques to Gmail are less secure. Only 50 percent of them encrypted while in transit, up from 27 percent in December.

Encryption reduces the chances that email can be read by interlopers. The technology transforms the text into coding that looks like gibberish until it arrives at its destination.

Google and other Internet services rely on a form of encryption known as Transport Layer Security, or TLS. Security experts say that encryption method isn't as secure as other options. But encryption that is tougher to crack is also more complicated to use.

Gmail, with more than 425 million accounts worldwide, was one of the first free email services to embrace TLS. Yahoo, Facebook and AOL also are encrypting their email services. Microsoft Corp., whose stable of email services includes the Outlook, MSN and Hotmail domains, has started encrypting many accounts as part of transition that won't be completed until later this year.

Less than half of the correspondence from Hotmail accounts to Gmail wasn't encrypted as of late May, Google said. Security is even worse at Comcast.net and Verizon.net, where less than 1 percent of the traffic coming to and from Gmail is encrypted, according to Google.

Comcast spokesman Charlie Douglas said the Internet service provider plans to start encrypting email to and from Gmail accounts within the next few weeks. Microsoft reiterated that it is still rolling out encryption in its free email services.

Verizon didn't have an immediate comment on Google's statistics.

The Google report comes a year after the first wave of media reports about the U.S. government's intrusive techniques to monitor online communications and other Internet activity. The National Security Administration says its online surveillance focused on people living outside the U.S. as the agency tried to defuse threats of terrorism.

After lashing out at the government spying, Google and other Internet companies began encrypting email and other online services in an attempt to reassure users worried about their privacy. The Internet companies are hoping their efforts to thwart government surveillance will make Web surfers feel comfortable enough to continue to visit their services. The companies make more money from online ads if their audiences keep growing.

Edward Snowden, the former NSA contractor who leaked documents revealing the online espionage, is among critics who believe the encryption methods deployed by Google and it peers are inadequate. In a March appearance at a technology conference, Snowden described TSL encryption as "deeply problematic" because U.S. government operatives merely needed to obtain a court order or hack into data centers to obtain users' emails and other information.

Like many privacy activists, Snowden prefers "end-

to-end" encryption, a more complicated step that requires a key to decrypt the information contained in emails. Theses encrypted keys are only held by an email recipient, making it virtually impossible for an unauthorized user to know what's in the message. This form of encryption takes more technical expertise to do right and can cause more headaches if passwords are forgotten because they can't be reset. That raises the risk of the email being inaccessible even to the recipient.

Google hopes to make end-to-end encryption easier by releasing an extension for its Chrome browser later this year. The company released the coding for the planned extension to security specialists Tuesday in an effort to detect any weaknesses before making it available to everyone.

More information:
www.google.com/transparencyreport/saferemail

APA citation: Volume of encrypted email rising amid spying fears (Update 2) (2014, June 3) retrieved 8 December 2021 from https://phys.org/news/2014-06-volume-encrypted-email-spying.html