Gmail's new 'confidential mode' offers more privacy controls—but don't get too comfortable

April 26 2018, by Jaclyn Cosgrove, Los Angeles Times

In rolling out major updates to Gmail, Google announced Wednesday that the popular email service will soon feature a new "confidential mode" that promises to give users more control over who sees the emails they send, and for how long.

Users should still be mindful about what they send over email, privacy experts warned, as messages sent in confidential mode could still fall into the wrong hands.

With the new privacy feature, users will be able to remove recipients' options to forward, copy, download or print specific messages.

"Useful for when you have to send sensitive information via email like a tax return or your Social Security number," Gmail product manager Matthew Izatt wrote in the company's announcement of the updates. "You can also make a message expire after a set period of time to help you stay in control of your information."

It probably would be easy to circumvent the confidential mode features, privacy experts pointed out: For example, a user might simply be able to take a screenshot or photo of an email they had been blocked from forwarding, or call over office mates to read the email from their screen. Google did not respond to an email raising those concerns.

Some online privacy experts, such as Sydney Li, staff technologist at the Electronic Frontier Foundation, argue that calling the new feature "confidential mode" is misleading. For one, Gmail's servers will still contain a copy of the email, Li said.

Other tech companies have dabbled with disappearing messages, most notably Snap Inc., whose Snapchat app faced some backlash in 2015 when users grew concerned that their app's new privacy policy suggested the company was keeping more of users' content than it had let on. "Don't send messages that you wouldn't want someone to save or share," it said.

Confidential mode will begin to roll out in the coming weeks, with a broader rollout to follow.

For the more than 4 million businesses that pay to use G Suite—an enhanced paid version of Google products such as Gmail, Docs and Calendar—confidential mode will include the option to require an email recipient to use a passcode, sent via text message, to view the email.

Li said this feature raises additional concerns because to use it, you might need to tell Google the recipient's phone number—potentially without the recipient's consent.

"This 'privacy' feature is potentially harmful to users with a real need for private and secure communications," Li said.

John Simpson, the privacy and technology director at advocacy group Consumer Watchdog, said enabling users to send emails that recipients cannot forward is a powerful tool, but it does raise the question of how people will get around it. Although Google might offer a confidential mode, there's only so much the tech giant can do to block human hijinks.

It's also unclear how the features will work when the email recipient is not a Gmail user. For example, Simpson said, is Gmail able to enforce a prohibition on forwarding if the recipient is using a different email service?

"It strikes me that people will be lulled into the feeling that this is a more confidential thing than is actually the case," Simpson said. "We need to see more about how exactly it's implemented, but clearly, if somebody went to the trouble to send me a message that I couldn't forward, and I looked at it, and said 'Holy mackerel! I want to show this to somebody else,' I think I could figure out ways to do it."

One aspect of confidential mode makes users more vulnerable to privacy breaches, the Electronic Frontier Foundation's Li said.

The feature that allows users to set a time limit on how long an email is available works by requiring the email's recipient to click a link to view the message, opening up a new attack opportunity for phishing, Li said.

"If people are trained to click on links in 'confidential' e-mails from other Gmail users, bad actors can send fake emails that resemble 'confidential' e-mails in order to trick users into clicking links that lead to phishing sites," Li said. "The phishing link could then present a fake Google login page, to try and steal the user's credentials."

Simpson, a longtime critic of Google, said that even as the company offers privacy enhancements, it is still looking out for itself.

Last year, Google announced it would stop using or scanning any Gmail content to help it personalize ads.

Simpson said that was a good move—but that Google made it primarily because it already collects enough information about users to target them with ads in line with their interests, and using email content wasn't even necessarily helping the company accomplish that goal. Before the change, if a friend sent a silly email, it would often produce bizarre related ads.

Integrating more features into Gmail keeps users on the Google product as long as possible, he said.

Confidential mode "is going to be presented by Google as all these wonderful features that customers are out there asking for, and that they're meeting customer demand, and while some of that may be true, it's necessary to remember it's also all about maximizing ways people will be enticed to continue to stay on Google's platform as much as possible so they can monetize your data, and when dealing with Google, one should never forget that," Simpson said.