

Google's new super-secure email is crazy strong but not for the forgetful

October 19 2017, by Elizabeth Weise, Usa Today



Credit: CC0 Public Domain

Google on Tuesday rolled out a nasty-complicated but insanely secure version of its Google accounts aimed at "those who need it most," such as journalists, politicians and activists. It's not pretty but stands a good

chance of keeping the bad guys out.

Called the Advanced Protection Program, it requires users to jump through a series of hoops most Internet companies have worked for years to make go away—dongles, extra passwords, locked-down systems that can't talk to anything else and a non-intuitive sign-up procedure.

This is so not plug-and-play.

What it is, however, is safe. Not "I work for the National Security Agency and print out the nuclear codes every time they change" safe, but more "I'm working on a Senate campaign and we really don't want the Russians, or anyone else, to get into our email system" safe.

Signing up requires a Google [account](#) and then linking not one but two dongles, or small devices that connects to a computer's USB port or via Bluetooth. Each produces a highly secure code key that uses the standards of the international FIDO Alliance (for Fast IDentity Online.)

These plastic keys are about the size of a regular door key but instead hold codes Google uses to verify that you're you and that you should have access to the account. The key can go into the USB drive on a computer or via Bluetooth to a mobile device such as a phone.

While the secure accounts are free, the hardware to make them secure costs money. A USB security key runs about \$25 while the Bluetooth-enabled keys are about \$18.

Once you've tied these keys to your Google account, you've got to have one of them present in order to access your mail and files.

Otherwise— take note—it's Do Not Pass Go, Do Not Collect Your Email.

"What I think has changed is that people recognize they may never be able to 'learn' how to act optimally in a defensive sense, so this program literally eliminates many sources of humans messing up," said Joseph Lorenzo Hall, chief technologist with the Washington D.C.-based non-profit the Center for Democracy & Technology.

That means using a locked-down Gmail account which may not have all the functionality a more open one could have, though Google does say it's exploring adding access to some trusted partners as time goes by.

And about that dongle? You really, really don't want to lose it, or forget your password. Google hasn't even said what the recovery process will look like, but it is expected take three to five days.

This isn't an email system for everybody, Hall said. Those who are considering it should think carefully about the threats they face before they sign on. For most regular email users it will be overkill.

But if someone's possibly being targeted by a nation state attacker or very determined attackers or organized criminals, the answer is a clear yes, he said.

"Sexual assault and domestic violence victims, billionaires, finance employees, judges and law enforcement officers—they certainly face these threats and should use it," he said.

The system also doesn't allow users the freedom that non-secure Google accounts have. Once signed up, their Google account is only able to gather data from a few secure apps so that miscreants can't get to their inbox or Google drive via them.

In a way, this is an admission of defeat but also of reality. The Holy Grail of online security has long been a system with serious security that

was as easy to use as any other program.

With the launch of Advanced Protection, Google is acknowledging that while no one has come up with something that's both easy to use and secure, there are enough people out there who really need protection that even a somewhat gnarly program is going to find users.

©2017 USA Today

Distributed by Tribune Content Agency, LLC.

Citation: Google's new super-secure email is crazy strong but not for the forgetful (2017, October 19) retrieved 9 April 2024 from <https://phys.org/news/2017-10-google-super-secure-email-crazy-strong.html>

<p>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.</p>
--