1. Your Name: Rob Baitinger
2. Describe the news item in 2-3 complete sentences: Google is rolling out new Gmail services for higher risk individuals that will feature opt-in policies including physical authenticator for logging into new location. According to the article author, it is largely in response to recent security hacks and events of last election.
3. Reference for the news item, typically a URL:

<https://www.usnews.com/news/technology/articles/2017-10-17/google-launches-advanced-gmail-security-features-for-high-risk-users>

1. **The Course topic this relates to the most:** Data Privacy/Security; multi-layered authentication
2. Publication Date: October 17 2017

# Google Launches Advanced Gmail Security Features for High-Risk Users

Oct. 17, 2017, at 7:15 a.m.

Google Launches Advanced Gmail Security Features for High-Risk Users

FILE PHOTO - The Google logo is pictured atop an office building in Irvine, California, U.S. August 7, 2017. REUTERS/Mike Blake/File Picture Reuters



By Dustin Volz

(Reuters) - Alphabet's Google Inc said on Tuesday it would roll out an "advanced protection program" to provide stronger email security for some users such as government officials, political activists and journalists who are at a higher risk of being targeted by sophisticated hackers.

Google users will have the ability to opt in to security settings aimed at protecting Gmail, Google Drive and YouTube data from phishing attacks.

The advanced protection features include an option to require a physical USB security key to connect to a desktop computer before each log-in as a way to verify a user's identity. Mobile log-ins will require a Bluetooth wireless device.

Advanced protection users will have their data walled off from access by any non-Google third-party applications, such as the Apple iOS mail client or Microsoft Outlook.

The program also includes a more laborious and detailed account recovery process to prevent fraudulent access by hackers who try to gain access by pretending they have been locked out.

Although Google has previously supported the use of security keys for what is known as two-factor authentication, advanced protection users will have no backup log-in method available if they lose their keys other than the fuller account recovery process.

Google did not specify what the recovery process would entail.

The rollout of a suite of new email security services follows a U.S. presidential election last year shaped in part by the disclosure of emails belonging to associates of Democratic candidate Hillary Clinton that were obtained through phishing schemes.

U.S. intelligence agencies have concluded that those hacks, which included a breach of Clinton campaign manager John Podesta's personal Gmail account, were carried out by Russia as part of a broader cyber campaign to help Donald Trump, a Republican, win the White House.

"If John Podesta had Advanced Protection last year, the world might be a very different place," said Joseph Lorenzo Hall, chief technologist at the Center for Democracy and Technology, who was briefed on the new features by Google.

Hall said the new features would increase the number of high-risk consumers with strong protections against phishing campaigns. But he noted that they may create compatibility issues among some who already integrate custom security tools with their Google products.

Google created a web page, g.co/advancedprotection, to walk users through setting up advanced protection, including where to purchase USB and Bluetooth security keys on Amazon .

(Reporting by Dustin Volz in Washington and Philip George in Bengaluru; Editing by Sunil Nair and Dan Grebler)