Google strengthens security system for all users

March 19 2020, by Peter Grad

Credit: CC0 Public Domain

Google announced today that it is bolstering its malware protection system for Google account holders. It will broaden the protective web provided by its Advanced Protection Program (APP) that has been offering additional security for high-profile users who face greater risks

of intrusions. Such users include celebrities, journalists, political figures, activists and business leaders, although anyone may access the program.

Google's Play Protect system daily scans more than 100 billion apps, including all apps installed on users' devices, for potential malware and other risks. It has been an option for users since its inception in 2017. But Google's move today will now require Play Protect by default and block users from turning it off.

Users will no longer be permitted to download apps from sources other than the Play Store, which will guarantee the integrity of app performance. Programs demanding access to Gmail or Drive data will be denied. Travel tracking apps commonly require such information.

Also, accessing Google services such as Gmail and Photos may now be done solely through Chrome and Firefox browsers.

There are exceptions though: Users may still use apps that came preinstalled on their phones. They may also use third-party platforms to download additional apps if those platforms were preinstalled on their phones.

In addition, advanced users will continue to have access to Android's Debug Bridge to enable selected third-party apps.

Popular programs such as Mail, Calendar and Contacts will not be affected by the new restrictions.

The AAP is available for free for anyone with a Google account. Users must have an Android 7.0+ or an iPhone 10.0 + with the free Google Smart Lock app. Users with other phone setups may obtain a Titan Security Key that enables protection at prices ranging from $25 to $40.

According to Google's APP information page, "Phishing is a common technique that can be used to trick you into giving away your username, password, 2-Step Verification code, or other personal information. Phishing attacks can happen through a variety of channels, including email, telephone, text message, or in apps… Security keys are the most secure form of 2-Step Verification.

With advanced protection, "even if you do fall for a phishing attack that discloses your username and password, an unauthorized user won't be able to access your account without one of your security keys."

Users may apply for Advanced Protection here: myaccount.google .com/ad … ection/landing?pli=1

More information: landing.google.com/advancedprotection/

Citation: Google strengthens security system for all users (2020, March 19) retrieved 3 February 2023 from https://techxplore.com/news/2020-03-google-users.html