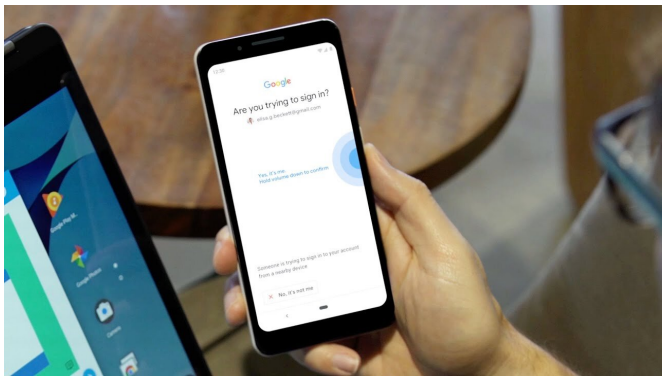
Google enables use of Android phones as a physical security key

11 April 2019, by Bob Yirka



Credit: Google

Google has announced that it has made software updates to Chrome and Android that make it possible to use an Android phone (7+) as a physical security key. In their announcement, Google once again claimed that using physical keys is the best way to counter phishing attacks, far better than messaging, for example.

In recent years, phishing attacks have become a major problem for users—many people have been fooled into revealing passwords and other credential information. Google and other technology companies have responded to this threat by making available physical security keys to users wishing for a second level of security. Such hardware devices have come down in price in recent years, but they are still inconvenient to use—they must be physically accessible when accessing an online account. Google has now made the same services possible without the need for such devices by allowing users to use their phone instead. The service is made possible through the use of Bluetooth communications technology.

In its announcement, Google outlined the two-step verification process and how to set it up on a computer and phone. The process is relatively simple—all users need to do is add their Google account to their phone if they have not done so already, enroll in the two-step verification program (2SV), adjust some settings, and then choose their phone from a list of options. It is also necessary to enable Bluetooth on both the phone and computer.

Once configured, the system provides two-step physical verification for user Google accounts, as well as Google Cloud accounts. Google strongly recommends that certain individuals take advantage of the service right away, including celebrities, journalists, and people working on political campaigns—anyone in the public eye who might make a prime target for a phishing attack.

Using the system is almost automatic—when logging into Google on their computer, a user will receive a notification on their phone asking them to verify the login. Once they do, the system will take care of the rest. Google also recommends registering a backup security key and keeping it somewhere where they will remember where it is in case their phone is lost or stolen.

More information:
www.blog.google/technology/saf … e-is-a-security-key/

gsuiteupdates.googleblog.com/2 … ecurity-key-2fa.html

APA citation: Google enables use of Android phones as a physical security key (2019, April 11) retrieved 22 April 2019 from https://techxplore.com/news/2019-04-google-enables-android-physical-key.html