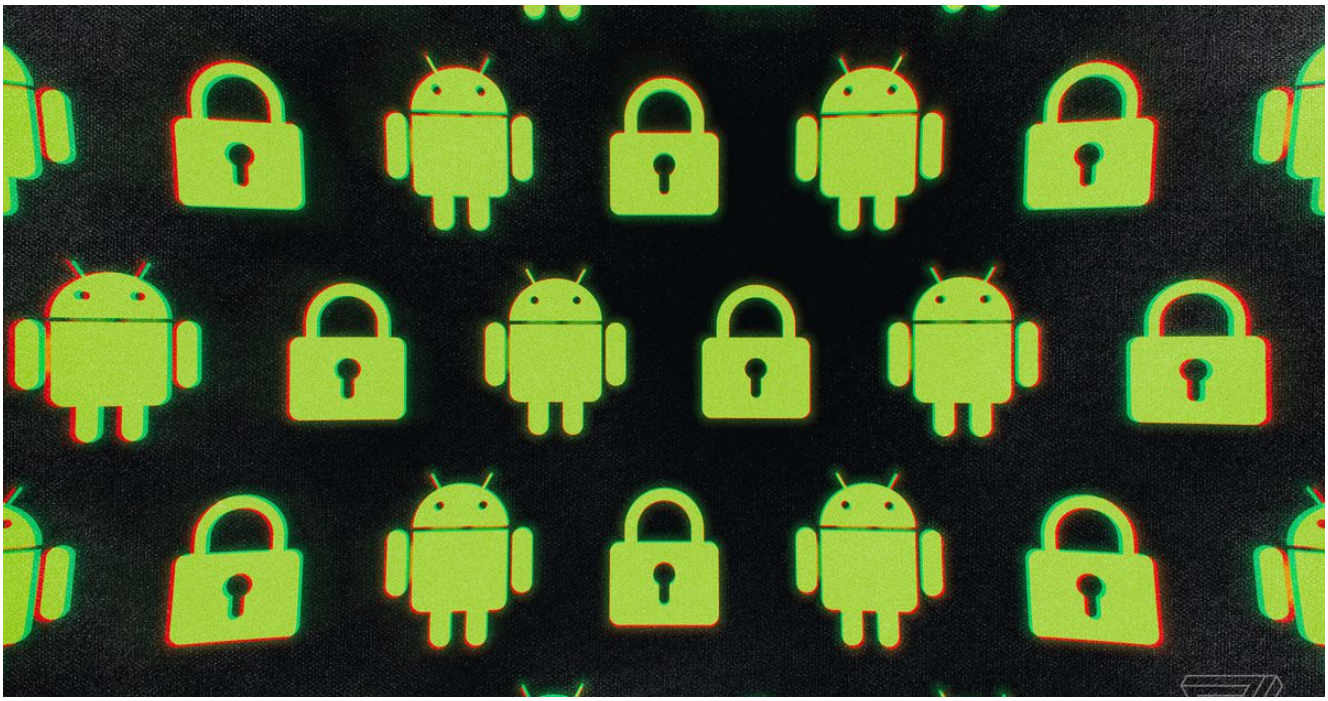
Google account hacks dropped by half after pushing two-step authentication by default



Nudging users toward security works.

That’s the top-line finding four months into Google’s initiative to enroll users in two-factor authentication by default, detailed in a blog post to coincide with Safer Internet Day on February 8th.

In October 2021, the company announced plans to turn on two-factor authentication by default for 150 million Google users who were not currently using the service and to require 2 million YouTube creators to use it. In the latest post, Google says it observed a 50 percent decrease in accounts being compromised among that test user group.

The strategy shows the power of a tech giant like Google to provide security by default and fits into a years-long project

to move users toward a more robust security model – eventually aiming at a future without passwords, according to another blog post published by the company last year.

Two-factor authentication, or "two-step verification" (2SV) as Google terms it, is a core pillar of this strategy, since account security is significantly increased by the requirement for a physical item like a security key, or phone to receive codes via app or SMS. But historically, the problem has been one of adoption.

"There is a lot of educating that needs to happen with 2SV"
In 2018, a Google engineer revealed that more than 90 percent of active Gmail accounts were not using two-factor authentication, prompting questions as to why Google wouldn't make the two-step authentication process mandatory. Since then, the company has been on a path to make 2SV a default option for a greater share of users and a mandatory step for some.

According to Google representatives, one of the remaining barriers is a lack of understanding about the full benefits of additional authentication procedures.

"There is a lot of educating that needs to happen with 2SV and we want users to understand what it is and why it's beneficial," said Guemmy Kim, director of account security and safety at Google.

"We also need to make sure that users' accounts are set up correctly with a recovery email and phone number so they can avoid account lockouts once 2SV is enforced. We've already enrolled users that we deem to be early adopters and whose accounts were 2SV ready," Kim said.

Although the number of web services supporting two-factor authentication has grown steadily, consumer adoption still remains low. Twitter, which rolled out two-factor authentication in 2013, revealed in 2020 that only 2.3 percent

of active accounts had enabled it; at Facebook, the figure was around 4 percent adoption in 2021.

Where adoption exists, the most common 2FA option is to send one-time codes via SMS – which security experts consider the method most vulnerable to interception. Ideally, two-factor authentication should make use of an authentication app, like Google Authenticator or Authy, or a physical device like a hardware security key.

https://www.theverge.com/2022/2/8/22923618/google-account-hacks-dropped-half-two-step-authentication