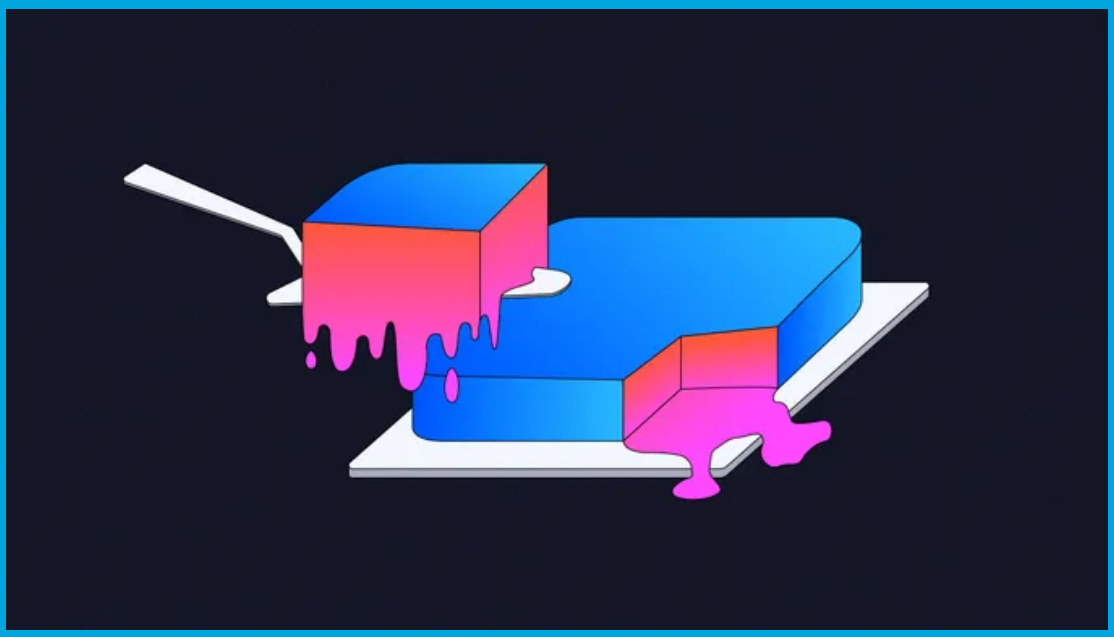
Security Newsletter

27 Feb 2023

Subscribe to this newsletter

You Can't Trust App Developers' Privacy Claims on Google Play



IT'S BASICALLY IMPOSSIBLE to keep track of what all your mobile apps are doing and what data they share with whom and when. So over the past couple of years, Apple and Google have both added mechanisms to their app stores meant to act as a sort of privacy nutrition label, giving users some insight into how apps behave and what information they may share. These transparency tools, though, are populated with self-reported information from app developers themselves. And a new study focused on the Data Safety information in Google Play indicates that the details developers are providing are often inaccurate.

Researchers from the nonprofit software group Mozilla looked at the Data Safety information of Google Play's top 40 most-downloaded apps and rated these privacy disclosures as "poor," "needs improvement," or "OK." The assessments were based on the degree to which the Data Safety information did or did not align with the information in each app's privacy policy. Sixteen of the 40 apps, including Facebook and Minecraft, received the lowest grade for their Data Safety disclosures. Fifteen apps received the middle grade. These included the Meta-owned apps Instagram and WhatsApp, but also the Google-owned YouTube, Google Maps, and Gmail. Six of the apps were awarded the highest grade, including Google Play Games and Candy Crush Saga.

"When you land on Twitter's app page or TikTok's app page and click on Data Safety, the first thing you see is these companies declaring that they don't share data with third parties. That's ridiculous—you immediately know something is off," says Jen Caltrider, Mozilla's project lead. "As a privacy researcher, I could tell this information was not going to help people make informed decisions. What's more, a regular person reading it would most certainly walk away with a false sense of security."

Read More

More #News

- Twitter gets rid of SMS 2FA for non-Blue members — What you need to do
- ChromeLoader campaign lures with malicious VHDs for popular games
- News Corp says state hackers were on its network for two years

#Breach Log

- GoDaddy: Hackers stole source code, installed malware in multi-year breach
- Atlassian data leak caused by stolen employee credentials
- Stanford University discloses data breach affecting PhD applicants

#Patch Time!

- Microsoft fixes bug offering Windows 11 upgrades to unsupported PCs
- Microsoft urges Exchange admins to remove some antivirus exclusions

#Tech and #Tools

- Dish Network goes offline after likely cyberattack, employees cut off
- Brave browser to block “open in app” prompts, pool-party attacks

This content was created by Kindred Group Security. Please share if you enjoyed!

Kindred Group in brief

Kindred Group is one of the world's leading online gambling operators with business across Europe, US and Australia, offering more than 30 million customers across 9 brands a great form of entertainment in a safe, fair and sustainable environment. The company, which employs about 2,000 people, is listed on Nasdaq Stockholm Large Cap and is a member of the European Gaming and Betting Association (EGBA) and founding member of IBIA (Sports Betting Integrity Association). Kindred Group is audited and certified by eCOGRA for compliance with the 2014 EU Recommendation on Consumer Protection and Responsible Gambling (2014/478/EU). Read more on www.kindredgroup.com.

You can access the previous newsletters at https://news.infosecgur.us