Policy Brief

Safeguarding The Unsuspecting User

Keeping fraudulent apps off app stores

June 2021

Authors: Shivani Gupta, Rohit Kumar

Context

Lately, several reports have highlighted the user impact of fraudulent apps. These apps pose a threat to India's growing smartphone user community, particularly due to limited understanding of digital safety. In such a situation, it becomes imperative for India to take the lead in creating user-friendly and safe app store ecosystems.

In the attached document, we present a detailed note on the due diligence processes deployed by the Google Play Store, an app store platform owned by Google. We delve deeper into the Play Store simply because of its large market share in the Indian context; the presence of fraudulent apps is otherwise a matter of concern for all app stores including the Apple App Store. Our research suggests that while app stores undertake several checks *before* listing an app on the platform, the checks deployed *after* an app is listed are limited. Several instances have been reported where apps that used bots as tools for impersonation, or violated user safety policies continued to be available on app stores for several years despite posing a risk to users. As a result, a large number of apps continue to commit cyber fraud often leading to grave consequences for users. This calls for the adoption of a more robust mechanism to keep fraudulent apps off app stores.

Keeping fraudulent apps off app stores

Instances of online fraud have rapidly increased over the last couple of years in India as more users have started using web-based services. On mobile phones, many unsuspecting users find themselves caught in fraudulent transactions while using apps specifically designed with malicious intent (called "fraudulent apps" here on). These apps, in addition to risking unsuspecting users, cause reputational damage to the app industry and pose a business risk to genuine app products by eroding user trust.

Google and Apple are the major distributors of apps through their app stores on mobile phones. In the Indian context, Google dominates the market - on the Android Operating System, 90% of all downloads are done through the Google Play Store[1] and Android's market share in the operating system market in India is 96.41% (January, 2021)[2]. Given its role in distribution and gatekeeping, this note primarily focuses on the due diligence exercised by Google while onboarding apps on its Play Store, while highlighting potential gaps that leave users at risk.

Google Play Store: Pre and post app listing checks

Google's policy explicitly states that it does not 'allow apps or app content that undermine user trust in the Google Play ecosystem.' This includes apps that reflect 'a pattern of harmful behavior or high risk of abuse'[3]. In doing so, it recognizes that one of the best ways to protect users from bad apps is to keep those apps out of the Play Store in the first place.

There are several checks carried out by the Play Store before listing an app. These include (but are not limited to) checking the app's privacy policy (to protect user information), content rating and ads for age appropriateness. However, the checks carried out by the Play Store while onboarding apps (see Appendix) may not fully succeed in keeping fraudulent apps off the Play Store. This is largely because app users have not been onboarded by the listing stage, and the Play Store review team may not be able to ascertain whether the app is going to use bots, onboard paid-pretend users or encourage fraudulent activities on the app in the future. There is also no rule in the Google Play Developer Distribution Agreement (DDA) that prevents chat or messaged-based apps from using bots/paid employees to impersonate real people. While Google's Developer Policies state that impersonation is not allowed, it is unclear if Google checks for impersonation and delists apps for doing so. Google's DDA states that it 'does not undertake an obligation to monitor the products or its contents'[4].

An App Defense Alliance was announced in 2019 to quickly find Potentially Harmful Applications (PHAs) *before* they go live on the Play Store and take appropriate action for user protection. PHAs are apps that could put users, user data or devices at risk and have been classified into 15 different malware categories. Violations include ad fraud, billing fraud, phishing, spam, etc. The Alliance is a collaboration between Google and other technology partners in the business of mobile device protection who use automated scanning and secure communication to alert each other about PHAs. The success metrics of this alliance have not been officially reported by Google yet, but Google's Transparency Report on the Android Ecosystem Security shows that while the percentage of PHA installs has come down over the last 12-month period, as of December 2020, India is the top country with PHA installs.

[1] CCI Order no. 7 of 2020, Page 26, paragraph 51
[2] Last accessed on February 28th, 2021: https://gs.statcounter.com/os-market-share/mobile/india
[3] https://support.google.com/googleplay/android-developer/answer/10146128?visit_id=637541587817223273-3537030883&rd=1
[4] Google Play Developer Distribution Agreement, Effective as of November 17th 2020, Paragraph 8.2:
https://play.google.com/about/developer-distribution-agreement.html

As per Google's Security Blog, in 2019, the Play Store stopped over 790,000 policy-violating app submissions before they were published to the Play Store[5]. In 2020, they prevented over 962,000 submissions from getting published on Google Play using their app vetting mechanisms and machine learning capabilities[6]. But, all of these are measures that are taken *before* an app is listed.

Once listed, the most effective way of identifying and flagging fraudulent apps to the Play Store is by 'reporting' them. However, users are more likely to leave a negative comment in the review section if they are unhappy with an app than report it[7].

In 2017, Google designed Play Protect as a built-in malware defense for Android phones. Similar to an antivirus software for a computer, Play Protect scans all of the apps on Android phones at frequent intervals to detect if the users have installed any harmful applications. However, the PHA scanning services continue to remain automated and based on machine learning models and often miss out on fraudulent apps that can only be pulled up through a manual review/ on the basis of complaints. This was recently noted when a developer was arrested for creating two fraudulent apps that allowed tatkal ticket bookings on the Indian Railways. These apps remained functional for a four-year period during which time they continued to offer confirmed train tickets to customers if they purchased 'coins' before booking. The apps were also in contravention of the provisions of the Railways Act, 1989.

Fraudulent apps and their impact on users

There have also been several other instances when the Play Store has only been able to act upon fraudulent apps once the damage has been done. In early 2021, the Ministry of Electronics & Information Technology asked Google to remove fraudulent personal loan apps from its Play Store. These apps were involved in misuse of users' personal data and unlawful practices of physical threats and use of coercive methods for loan recovery. In a blog post, Google said that after receiving information from government and users, it scanned hundreds of personal loan apps in India, many of which were found to be violating their user safety policies[8]. Surprisingly, these apps continued to exist on the platform despite clear violation of Play Store policies that financial services apps offering personal loans are required to abide by[9]. This suggests that without aggressive monitoring of existing apps on the Play Store, it is likely that Google's systems miss apps that lead to user harm.

Similarly, in late 2020, Google removed three apps meant for children (with over 20 million downloads collectively) when they were flagged by the International Digital Accountability Council (IDAC), a Boston-based non-profit created to improve digital accountability. These apps were found to be violating Google's user data policies and yet, were allowed to operate, and acquire a large user base on the Play Store[10].

While Apple's App Store has a miniscule user base in India in comparison to Google's Play Store, recent lawsuits filed against the company in the United States bring to light the insufficiency of the app review mechanisms deployed. App developers in the US have been fighting a public battle against the tech giant for allowing apps that clone popular apps. These fraudulent apps are often found to be non-functional copycats of the popular versions and charge exploitative subscription fees to unsuspecting users, while getting away with the fraud because of fabricated reviews and ratings on the App Store[11].

[5] https://security.googleblog.com/2020/02/how-we-fought-bad-apps-and-malicious.html
[6] https://security.googleblog.com/2021/04/how-we-fought-bad-apps-and-developers.html
[7] Inputs from stakeholder conversations.
[8] Google India blog post, January 14th 2021: https://india.googleblog.com/2021/01/
[9] https://support.google.com/googleplay/android-developer/answer/9876821?hl=en
[10] https://techcrunch.com/2020/10/23/google-removes-3-android-apps-for-children-with-20m-downloads-between-them-over-data-collection-violations/
[11] https://www.theverge.com/2021/2/8/22272849/apple-app-store-scams-ios-fraud-reviews-ratings-flicktype

The issue of fraudulent and malicious apps has also come up in the ongoing Epic Games v. Apple antitrust lawsuit in the United States. Epic has cited Apple's internal documents where Apple's officials have spoken about the insufficiency of App Store's review processes in preventing fraudulent apps from making it to the app store[12], [13].

Building robust oversight mechanisms for app stores

Bad user experience due to the presence of fraudulent apps on the app stores should not only be a business concern for the app developer community but also for distributors like Google and Apple. Fraudulent apps also present a grave risk to millions of Indians, especially newer users who have only recently started participating in the digital economy and have limited understanding of online safety.

As intermediaries under the Information Technology Act, 2000, app stores are required to undertake due diligence and also have a grievance redressal mechanism to address complaints[14]. While app stores offer several checks prior to and post listing of apps, given the above examples of fraudulent apps (of which there are many in other jurisdictions as well[15], [16], [17]) there is a case for all app stores to explore additional measures and work closely with their community to ramp up monitoring mechanisms to proactively detect and remove bad actors to protect users from fraudulent apps. In high-risk use cases like lending, an approach that involves whitelisting or certification by regulators can also be pursued.

[12] https://appleinsider.com/articles/21/04/08/epic-lays-out-its-case-as-the-injured-party-in-dispute-with-apple-that-it-created

[13] https://appleinsider.com/articles/21/05/06/phil-schiller-showed-concern-about-scam-apps-as-early-as-2012

[14] Ministry of Electronics and Information Technology Notification on the Intermediary Guidelines, February 25th 2021, Page 21: https://www.meity.gov.in/writereaddata/files/Intermediary_Guidelines_and_Digital_Media_Ethics_Code_Rules-2021.pdf

[15] https://www.deccanherald.com/specials/google-removes-5000-ad-fraud-android-apps-from-play-store-880419.html

[16] https://thehackernews.com/2021/04/over-750000-users-download-new-billing.html

[17] https://www.businessinsider.in/cryptocurrency/news/167-fake-cryptocurrency-and-trading-apps-used-by-hackers-to-steal-money-sophos-exposes/articleshow/83138720.cms

APPENDIX - Due diligence on the Google Play Store

Table 1 lists the different kinds of systems and processes in place that developers have to go through to be able to list their apps on the Play Store. The table highlights the 'checks' carried out by the Play Store team at any of the stages prior to listing of an app on the Play Store. Even if Google's review process describes a minimal oversight of what is allowed/not allowed at a certain stage, that has been marked as a check (✓) in the table below. However, it is important to keep in mind that it is difficult to ascertain how stringent this check is, especially since apps aren't fully functional at the review stage.[18]

Table 1: Checks by Google Play Store prior to listing apps[19]

S.No.	Activity	Any check?	Description	Comments
1.	Creating a Developer Account	**?**	Anyone with a Gmail account can pay the one-time $25 registration fee and set up a developer account	In its 2019 White Paper[20], Google says that a review based on developer's 'profile and credit cards' is conducted when developers register via this form. It is unclear if Google uses past records of malicious developer accounts to conduct this review.
Preparing an app for review				
2.	Adding app details and descriptions	✓	Screenshots of app interface shared at the time of listing should match the app interface, as seen by Google's team at the time of app review.	
3.	Privacy Policy	✓	Adding a privacy policy is optional but if an app requires sensitive permissions or data[21] or is designed for families, a privacy policy is mandatory.	It is understood that it is usually better to include a privacy policy while listing an app, failing which some parts of the app tend to get disapproved by the review team[22].

[18] Updates are also subject to review. Anecdotally, we know that these reviews take a short amount of time (2 hours) and thus may only be restricted to the updated sections of the app.

[19] https://support.google.com/googleplay/android-developer/answer/9859455?hl=en

[20] Android Enterprise Security White Paper (Updated January, 2020), Page 21, Last accessed on April 30th, 2021: https://static.googleusercontent.com/media/www.android.com/en//static/2016/pdfs/enterprise/Android_Enterprise_Security_White_Paper_2019.pdf

[21] Including but not limited to personally identifiable information, financial and payment information, authentication information, phonebook, contacts, device location, SMS and call related data, microphone, camera. For more information, refer to Google's User Data Policy.

[22] Inputs from stakeholder conversations.

4.	Ads	✓	Deceptive, disruptive and inappropriate ads are not allowed.	Eg. Deceptive ads - Ads must not simulate or impersonate the user interface of any app, notification, or warning elements of an operating system. Eg. Inappropriate ads - The ads in the app must be appropriate for the intended audience of the app.
5.	Target audience and content	✓	Depending on the target audience selections, an app may be subject to additional Google Play policies.	Apps that are specifically designed for children under 13, and those designed for *everyone*, including children must comply with Google's Families Policy Requirement. This policy ensures that apps accessible to children show appropriate content, suitable ads, and handle personal and sensitive information correctly. It is the developer's responsibility to ensure that their app complies with all relevant laws[23]. Apps that are meant for mature audiences but may unintentionally appeal to children are required to carry the "Not designed for children" label in their app store listing[24].
6.	Permissions Declaration Form	✓	A developer may not request permissions that give access to user or device data for undisclosed, unimplemented, or disallowed features or purposes. This includes permissions related to SMS and call logs, location and files.	

[23] https://support.google.com/googleplay/android-developer/topic/9877766#!?zippy_activeEl=families-policy%23families-policy

[24] https://support.google.com/googleplay/android-developer/answer/9867159#declare_target_age_group&zippy=%2Coverall-best-practices%2Cage-and-under%2Cages-and-over

7.	Content Ratings Questionnaire	✓	This questionnaire, filled in by the developers, is used to signal to users what the suitable target audience for the app is, in terms of age appropriateness. Google Play uses multiple rating authorities (depending on local regulations) for this purpose and each authority's rating may vary depending on their own methodology. Unrated apps may be taken off the Play Store.	These ratings reflect the intended audience and are meant to serve as guidance, especially to parents, to identify apps that may contain potentially objectionable content. Developers answer specific questions about the app's content in this questionnaire, particularly with respect to content on violence, sexuality, language, crime or adult-oriented content. Ratings may vary be territory.
Submitting an app for review				
9.	App goes to review team	✓	An automated application risk analyser checks for potentially harmful app behaviour. When the risk analyser detects somethings suspicious, a human reviewer is pulled in for a manual review[25]. Reviewer will use the credentials shared by the developer to access any locked/purchase-based sections of the app. The app is checked for compliance with Play Store policies and the areas discussed under 'Preparing an app for review' section (Pts. 2-8).	Note that it may be difficult for Google to ascertain the fraudulent nature of the app at this stage when users have not been onboarded. **For instance, in the case of a dating app, Google Play is more likely to review the app as a 'chat' or a 'messaging' app, and thus any fraudulent elements such as use of bots or impersonation of other users by paid employees will not be detected at this stage.** This can probably only be identified through complaints or monitoring post-publishing[26].

[25] Android Enterprise Security White Paper (Updated January, 2020), Page 21, Last accessed on April 30th, 2021: https://static.googleusercontent.com/media/www.android.com/en//static/2016/pdfs/enterprise/Android_Enterprise_Security_White_Paper_2019.pdf

[26] Through conversations with developers with 5+ years of listing apps on the Play Store, we know that while earlier apps used to be approved for listing within 2-3 hours, the process now takes 2-3 days. This may be a result of Google using 'humans, not bots to reviews decisions on the Play Store'.: https://android-developers.googleblog.com/2019/04/improving-update-process-with-your.html#my_anchor