How we keep harmful apps out of Google Play and keep your Android device safe

February 2016

android

Bad apps create bad experiences, so we work hard to keep them off your device and out of Google Play. In 2015, bad apps were installed on less than 0.13% of all devices that only install apps from Google Play. Before an app appears on Google Play, it is reviewed and tested for safety and security. This document describes some of the ways we review for and detect apps that pose a security risk for users or their data. We refer to such apps as Potentially Harmful Applications.

Some categories of Potentially Harmful Applications:

Hostile Downloader
Apps that are not harmful by themselves, but they download other potentially harmful applications

Phishing
Apps that mask themselves as trustworthy, then request authentication credentials or billing information, which they share with a third party

Backdoor
Apps that can let people control your device without your approval

Spyware
Apps that quietly track what you do on your device, then send that information to a third party

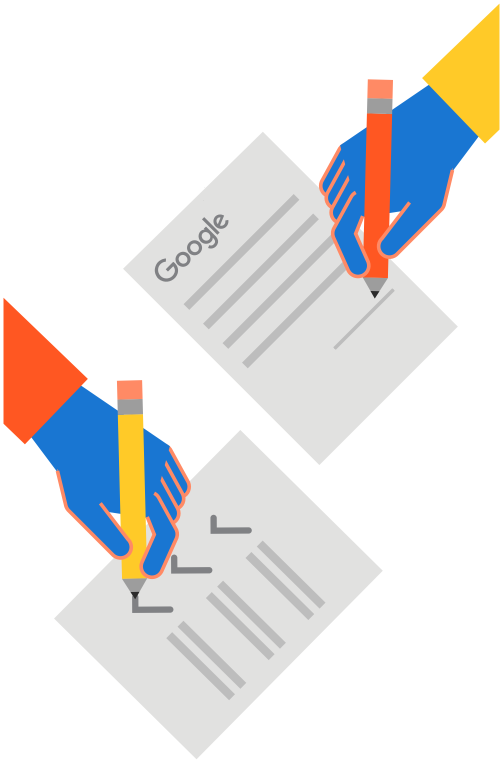
Ransomware
Apps that hold you hostage by doing things like locking you out of your device or encrypting data and then demanding payment

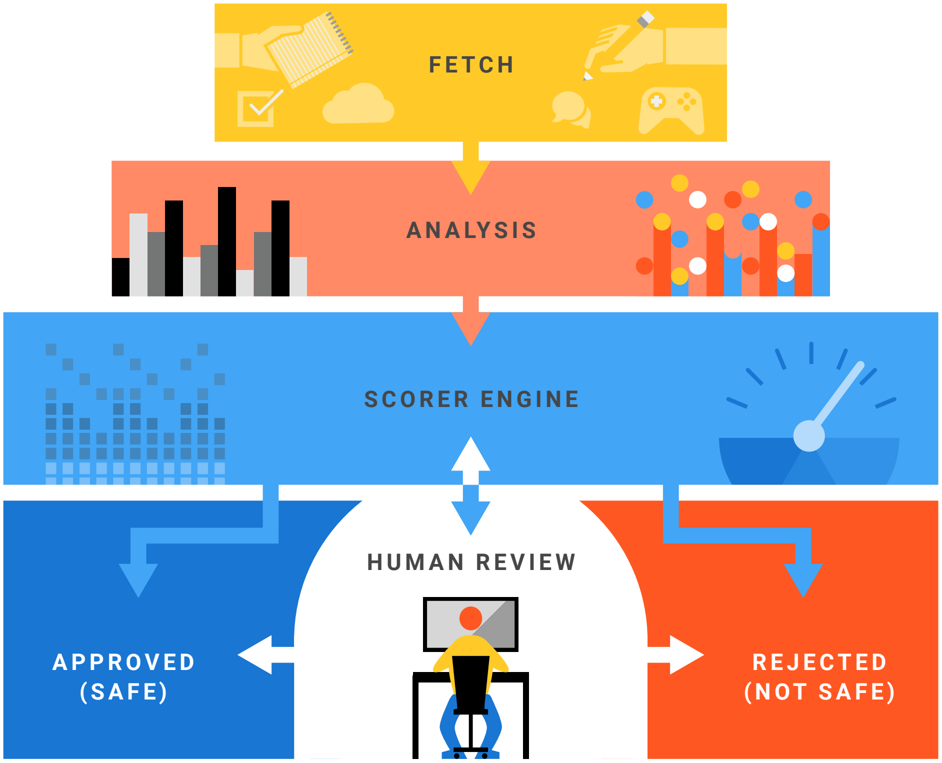
Before you install an app from Google Play

We start working on your safety before you ever install an app from Google Play. To do so, we review both developers and apps before they are allowed in the Play store.

We check all developers
Before a developer can submit their app on Google Play, they must agree to the Google Play Developer Distribution Agreement (DDA). This contract guides developer behavior to ensure that apps on Google Play are safe and can be trusted.

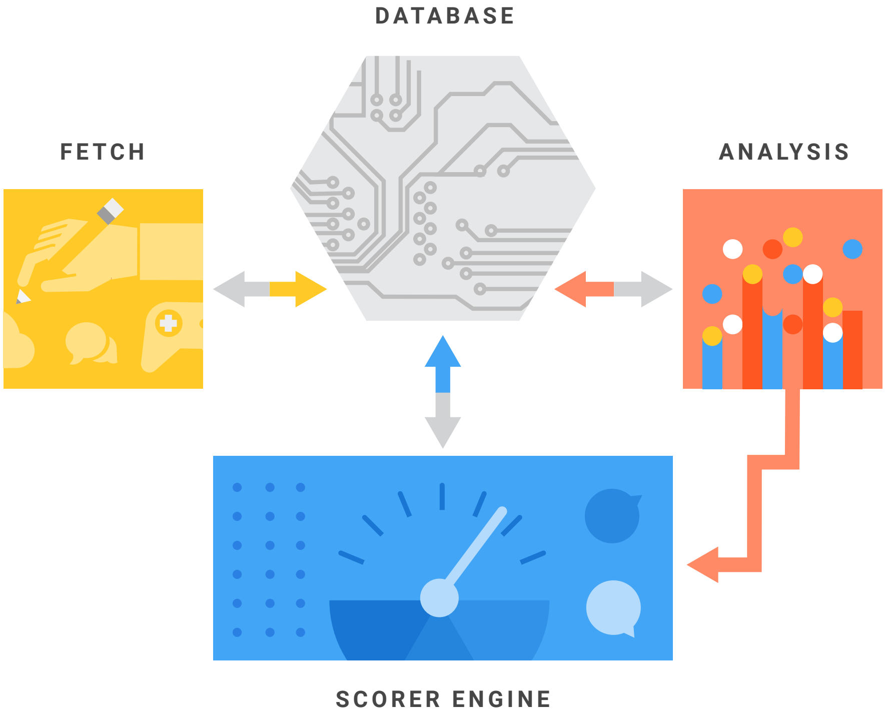
Additionally, Google Play uses a variety of methods to work to check that developers are complying with these policies. One example is Google Play's internal risk engine, which analyzes various signals about a developer's Google account, actions, history, billing details, device information, and more. If something suspicious turns up, we manually review the transactions to ensure that the developer is compliant.





We review all apps
Once a developer has been reviewed and approved, they can submit their app to the Google Play Store. Before that app is made available to you, it goes through a variety of reviews in our security-detection system.

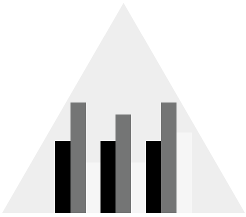
Fetch app samples
In addition to apps submitted by developers, we continually fetch new samples from diverse and numerous sources. Some apps are submitted by security researchers, reported by users, and others we find by crawling the internet and inspecting installed apps from other markets. Thanks to these various sources, our security system processes over 400k apps each day.



Analyze for harmful apps

To process all of this information, our security-detection system uses advanced techniques like machine learning to see patterns and make connections that humans otherwise would not. These signals and results from the system are continuously monitored and refined to reduce error rate and improve precision. As our system learns new signals, it reevaluates previously scanned Android apps to make sure they are still safe. These signals are also reviewed alongside developers’ information.

Some of the ways that our machines learn what is good and what is bad:

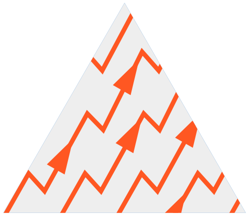


Static Analysis

We analyze application code without running the app. Application features are extracted and analyzed against expected good behavior and potential bad behavior.

Dynamic Analysis

We run applications to identify interactive behavior that cannot be seen with static analysis. This allows reviewers to identify attacks that require connection to a server and dynamic downloading of code.

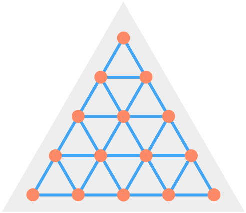


Heuristic and Similarity Analysis

We compare applications with each other to find trends that lead to harmful apps.

Signatures

We use signatures to compare apps against a database of known bad apps and vulnerabilities.

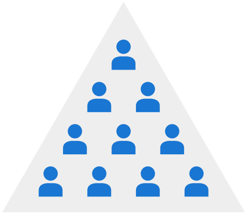


SafetyNet

A privacy preserving sensor network spanning the Android ecosystem, identifying apps and other threats that cause harm to the device.

Third-party Reports

We cultivate active relationships with industry and academic security researchers.These independent security researchers also evaluate applications in a variety of ways and will often let us know if they see something amiss.



Developer Relationships

We analyze non-code features to determine possible relationships between applications and to evaluate whether the developer that created the application may have previously been associated with creation of potentially harmful applications.

Score the apps

After we analyze the apps, they are classified on a scale of safe to harmful. Apps and app updates that are marked as safe go straight to Google Play. Apps that are marked as harmful are blocked. And apps that are somewhere in the middle are marked as potentially harmful. Potentially harmful applications are manually reviewed by members of the Android Security Team.

Developers who knowingly perform malicious actions are banned and no longer allowed to publish apps on Google Play. Of course, developers may provide additional information if they disagree with a decision, and we will evaluate their request.

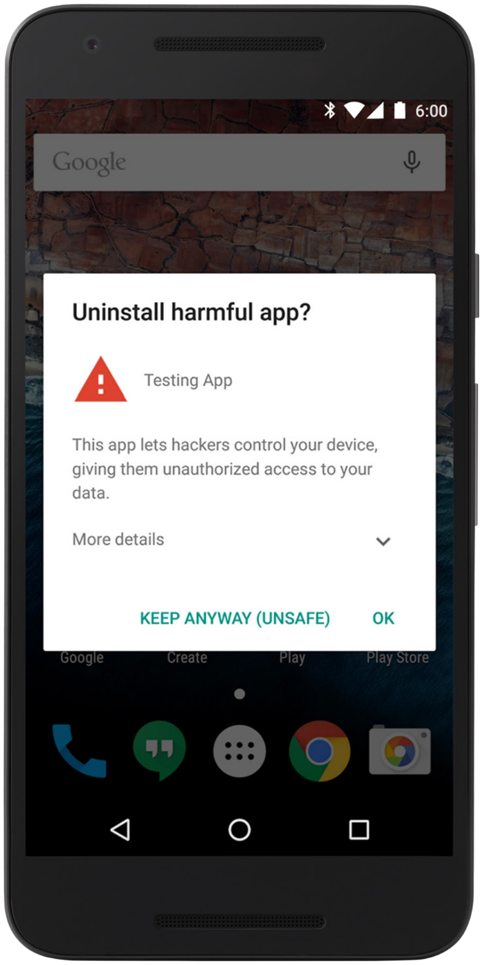
After you install an app

Even though we do a lot of work to make Google Play apps safe before they reach you, Google works hard to protect you—no matter where your app comes from. We sandbox each application to constrain bad behavior and if an app wants new permissions, we ask you to confirm at runtime.

In addition to multiple layers of security built into the platform, Android also includes a feature called Verify Apps. Verify Apps continually scans for potentially harmful apps. If an app is discovered later to be potentially harmful, Verify Apps will disable the app and request for you to remove it.

Verify Apps also checks apps you install from outside of Google Play. If we see an app that looks malicious, we warn you before the installation proceeds. Verify Apps is available on every Android device (2.3+) that has Google Play installed.

With SafetyNet, security sensitive events and settings changes are used as signals to identify suspicious app behavior across the Android ecosystem. For example, attempts to send SMS to premium services without user consent are logged and analyzed to identify potentially harmful apps. SafetyNet also observes attempts by apps to exploit known vulnerabilities, allowing our systems to classify such apps as dangerous and subsequently block their installation with Verify Apps.



Uninstall harmful app?

Testing App

This app lets hackers control your device, giving them unauthorized access to your data.

Conclusion

Google works to keep your devices safe from all angles. Google Play reviews developers and applications before they come to your devices, and continually updates its security-detection system to learn more ways to keep harmful applications away. Android has multiple layers of built-in security, like Verify Apps, SafetyNet, sandboxing, and runtime permissions.

We’re working hard to make sure your device never meets a harmful application. But it’s not just us—we are constantly collaborating with developers, academic and industry researchers, and users like you to make Google Play and Android safe. Download with confidence: we’re all on your side.