Mobile Unwanted Software (MUwS)

At Google, we believe that if we focus on the user, all else will follow. In our Software Principles (https://www.google.com/about/software-principles.html) and the Unwanted Software Policy (https://www.google.com/about/unwanted-software-policy.html), we provide general recommendations for software that delivers a great user experience. This policy builds on the Google Unwanted Software Policy by outlining principles for the Android ecosystem and the Google Play Store. Software that violates these principles is potentially harmful to the user experience, and we will take steps to protect users from it. This information is also available on android.com (https://www.android.com/mobile-unwanted-software-policy/).

As mentioned in the Unwanted Software Policy (https://www.google.com/about/unwanted-software-policy.html), we've found that most unwanted software displays one or more of the same basic characteristics:

- It is deceptive, promising a value proposition that it does not meet.
- It tries to trick users into installing it or it piggybacks on the installation of another program.
- It doesn't tell the user about all of its principal and significant functions.
- It affects the user's system in unexpected ways.
- It collects or transmits private information without users' knowledge.
- It collects or transmits private information without a secure handling (for example, transmission over HTTPS).
- It is bundled with other software and its presence is not disclosed.

On mobile devices, software is code in the form of an app, binary, framework modification, etc. In order to prevent software that is harmful to the software ecosystem or disruptive to the user experience we will take action on code that violates these principles.

Below, we build on the Unwanted Software Policy to extend its applicability to mobile software. As with that policy, we will continue to refine this Mobile Unwanted Software policy to address new types of abuse.

Transparent behavior and clear disclosures

All code should deliver on promises made to the user. Apps should provide all communicated functionality. Apps should not confuse users.

- Apps should be clear about the functionality and objectives.
- Explicitly and clearly explain to the user what system changes will be made by the app. Allow users to review and approve all significant installation options and changes.
- Software should not misrepresent the state of the user's device to the user, for example by claiming the system is in a critical security state or infected with viruses.
- Don't utilize invalid activity designed to increase ad traffic and/or conversions.
- We don't allow apps that mislead users by impersonating someone else (for example, another developer, company, entity) or another app. Don't imply that your app is related to or authorized by someone that it isn't.

Example violations:

- Ad fraud
- Impersonation

Protect user data

Be clear and transparent about the access, use, collection, and sharing of personal and sensitive user data. Uses of user data in must adhere to all relevant User Data Policies, where applicable, and take all precautions to protect the data.

- Provide users an opportunity to agree to the collection of their data before you start collecting and sending it from the device, including data about third-party accounts, email, phone number, installed apps, files, location, and any other personal and sensitive data that the user would not expect to be collected.
- Personal and sensitive user data collected should be handled securely, including being transmitted using modern cryptography (for example, over HTTPS).
- Software, including mobile apps, must only transmit personal and sensitive user data to servers as it is related to the functionality of the app.

Example violations:

- Data Collection (cf Spyware (https://developers.google.com/android/play-protect/phacategories#spyware))
- Restricted Permissions abuse

Example User Data Policies:

- Google Play User Data Policy (https://play.google.com/about/privacy-security-deception/user-data/)
- GMS Requirements User Data Policy (https://support.google.com/androidpartners_gms/answer/7351400)
- Google API Service User Data Policy (https://developers.google.com/terms/api-services-user-data-policy)

Do not harm the mobile experience

The user experience should be straightforward, easy-to-understand, and based on clear choices made by the user. It should present a clear value proposition to the user and not disrupt the advertised or desired user experience.

- Don't show ads that are displayed to users in unexpected ways including impairing or interfering with the usability of device functions, or displaying outside the triggering app's environment without being easily dismissable and adequate consent and attribution.
- Apps should not interfere with other apps or the usability of the device.
- Uninstall, where applicable, should be clear.
- Mobile software should not mimic prompts from the device OS or other apps. Do not suppress alerts to the user from other apps or from the operating system, notably those which inform the user of changes to their OS.

Example violations:

- Disruptive ads
- Unauthorized Use or Imitation of System Functionality

For more details about each content violation, review policy requirements on the Play Policy Center (https://play.google.com/about/developer-content-policy/), GMS requirements (https://docs.partner.android.com/gms/policies/overview/gms-requirements#mba-impersonation), and Google Play Protect (https://developers.google.com/android/play-protect/phacategories).

Mobile Unwanted Software (MUwS) categories

Data collection and restricted permissions abuse

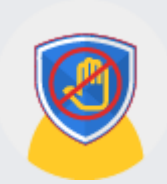
An app that collects and transmits personal and sensitive user data without adequate notice or consent. This may include collecting the list of installed apps, the device phone number, email addresses, location, or other third-party account IDs, or other personal information.

Social Engineering

An app that pretends to be another app with the intention of deceiving users into performing actions that the user intended for the original trusted app.

Disruptive ads

An app that shows ads that are displayed to users in unexpected ways including impairing or interfering with the usability of device functions, or displaying outside the triggering app's environment without adequate consent and attribution.



Unauthorized Use or Imitation of System Functionality

Apps or ads that mimic or interfere with system functionality, such as notifications or warnings. System level notifications may only be used for an app's integral features.

Ad fraud

Ad fraud is strictly prohibited. Ad interactions generated for the purpose of tricking an ad network into believing traffic is from authentic user interest is ad fraud, which is a form of invalid traffic (https://support.google.com/admob/answer/3342054?ref_topic=2745287). Ad fraud may be the byproduct of developers implementing ads in disallowed ways, such as showing hidden ads, automatically clicking ads, altering or modifying information and otherwise leveraging non-human actions (such as spiders and bots) or human activity designed to produce invalid ad traffic. Invalid traffic and ad fraud is harmful to advertisers, developers, and users, and leads to long-term loss of trust in the mobile Ads ecosystem.

Here are some examples of common violations:

- An app that renders ads that are not visible to the user.
- An app that automatically generates clicks on ads without the user's intention or that produces equivalent network traffic to fraudulently give click credits.
- An app sending fake installation attribution clicks to get paid for installations that did not originate from the sender's network.
- An app that pops up ads when the user is not within the app interface.
- False representations of the ad inventory by an app, for example, an app that communicates to ad networks that it is running on an iOS device when it is in fact running on an Android device; an app that misrepresents the package name that is being monetized.

Last updated 2020-10-30 UTC.