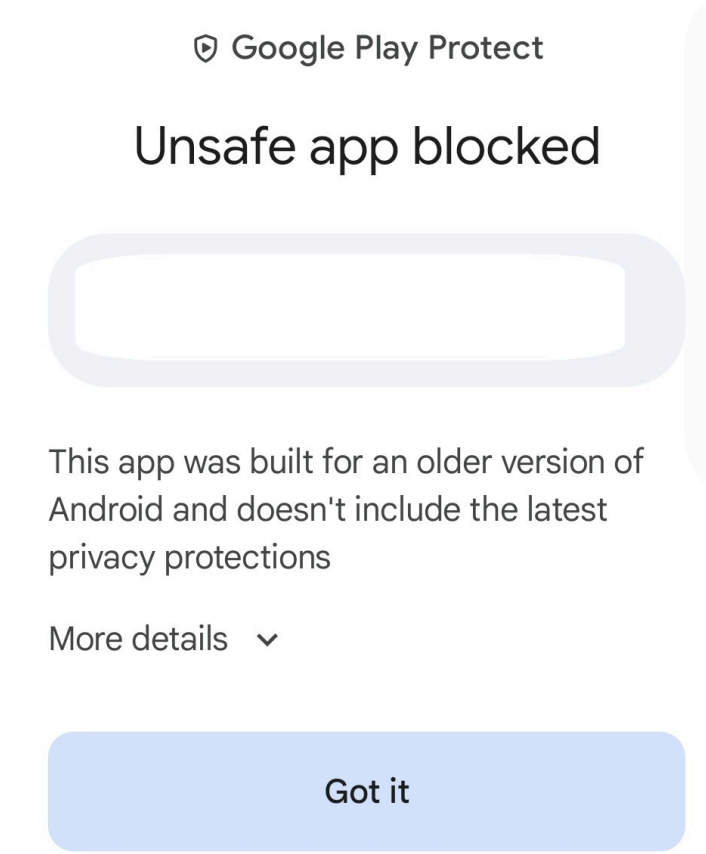
نسخه چاپی

خطای Blocked By Play Protect

Google Play Protect یک سرویس امنیتی جامع برای دستگاه‌های اندرویدی است که از کاربران در برابر برنامه‌های مخرب و بدافزارها محافظت می‌کند. این سیستم برنامه‌ها را صرف‌نظر از اینکه از Google Play یا سایر منابع نصب شده باشند، بررسی می‌کند.

در صورتی که توسعه‌دهنده‌ی برنامه‌ای هستید و برای یک بار نیز با خطای زیر مواجه شده‌اید، حتما این مقاله می‌تواند برای شما مفید باشد.

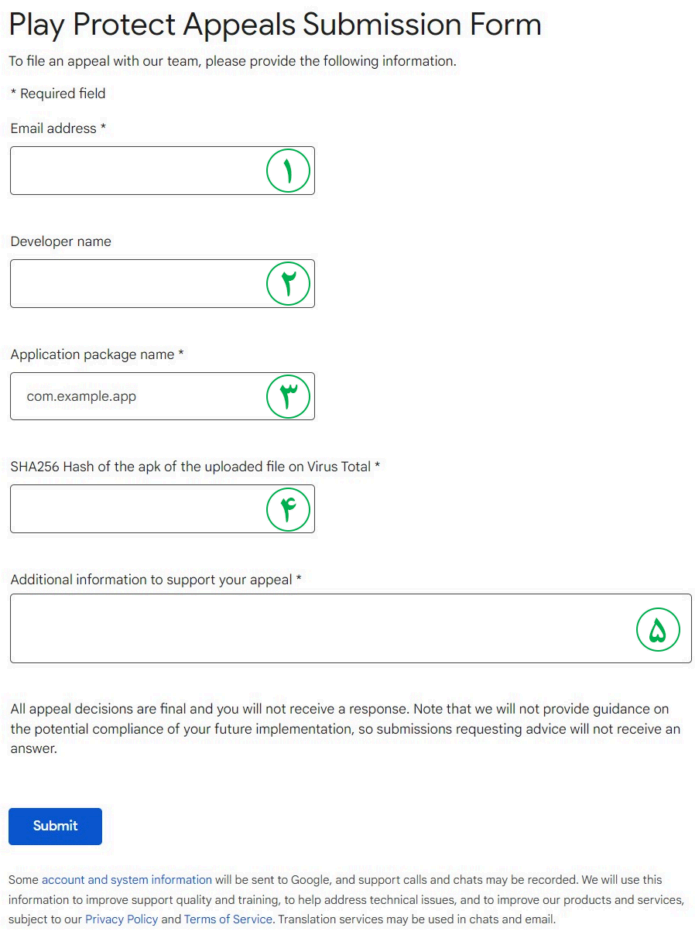


رفع مشکل خطای Blocked By Play Protect

ارسال فرم Play Protect Appeals:

برای حل خطای Blocked by Play Protect فرمی از سمت گوگل ارائه شده است که با تکمیل و ارسال آن می‌توانید نسبت به رفع این خطا اقدام کنید. می‌توان گفت، ارسال فرم، بهترین و تضمینی ترین راه برای حل این مشکل است. برای شروع لطفا با استفاده از برنامه تغییر IP، IP سیستم خود را تغییر داده و به صفحه Play Protect Appeals مراجعه و گام به گام توضیحاتی‌که در ادامه ارائه شده است، موارد فرم را تکمیل کنید:

لطفا به این مورد توجه داشته باشید که برای مشاهده‌ی فرم Play Protect Appeals لازم است تا حتما از ابزار تغییر IP استفاده کنید؛ در غیر اینصورت فرم قابل مشاهده نیست.



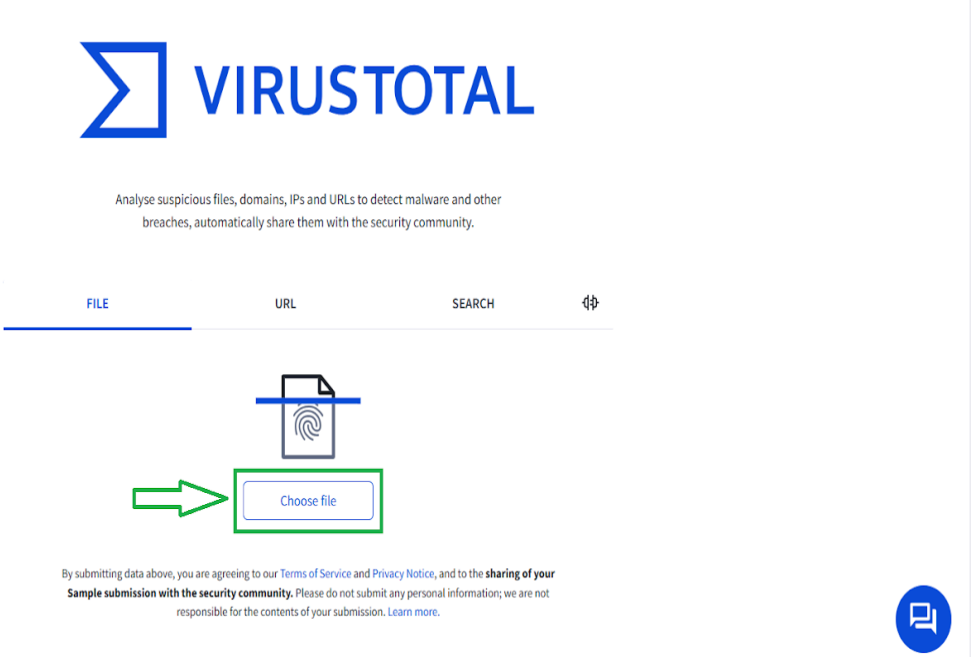
مراحل ایجاد درخواست

۱- Email Address: در اولین بخش فرم از شما آدرس ایمیل خواسته شده است، شما می‌توانید از هر آدرس ایمیلی که در دسترس دارید، در این بخش ثبت کنید.

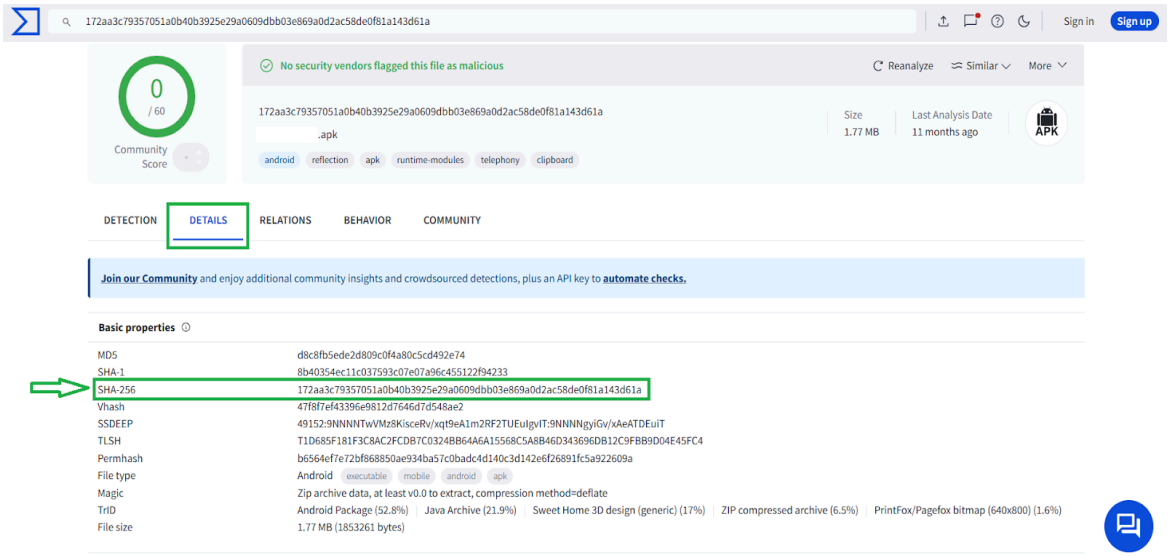
۲- Developer Name: نام توسعه‌دهندگی خود را در این بخش عنوان کنید.

۳- Application Package Name: نام بسته‌ی برنامه‌ای که با این خطا مواجه می‌شود را اعلام کنید.

۴- SHA256 Hash of the apk of the uploaded file on Virus Total: در این بخش لازم است شما به سایت Virustotal مراجعه کرده و بسته‌ی برنامه (APK) را طبق مراحل زیر بارگذاری کنید:



بعد از بارگذاری فایل لازم است تا، بر روی گزینه‌ی Details کلیک کنید و رشته 64 کاراکتری که در بخش رو به روی SHA-256 نوشته شده است را copy کرده و در بخش چهارم فرم گوگل قرار کنید.



۵- Additional information to support your appeal:

در این بخش باید توضیحی در مورد برنامه، حریم خصوصی کاربران و دسترسی‌ها به زبان انگلیسی بنویسید. که در ادامه یک متن به عنوان نمونه برای شما قرار گرفته است:

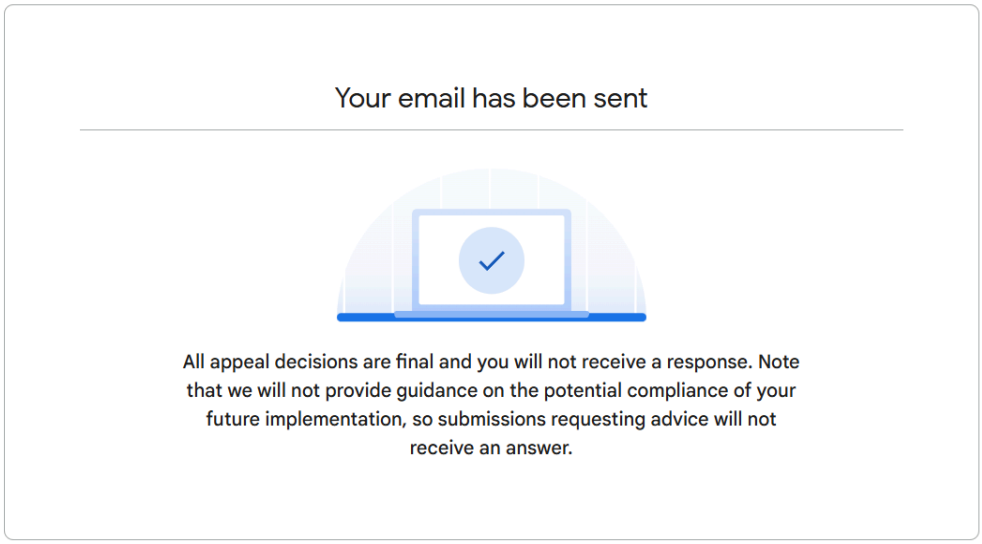
.Hi
This app is designed with the goal of [briefly explain the main objective of the app, such as .... "enhancing user productivity" or "facilitating communication"] and allows users to (در ادامه باید عملکرد برنامه خود را توضیح دهید)
:Key Features of Our App

We are committed to complying with all Google Play policies and regulations, and we are confident that our app meets all necessary requirements. Our goal is to provide a positive and .beneficial experience for users

In conclusion, we kindly ask you to reconsider our app and provide us with an opportunity to serve our users better. We appreciate your support and hope to contribute positively to our .user community

.Thank you for your attention
,Best regards

بعد از تکمیل فرم مربوطه در سایت گوگل تصویر زیر برای شما به نمایش درخواهد آمد:



در بعضی موارد ممکن است که از سمت گوگل تاییدی دریافت نکنید، اما این به معنای صحیح تکمیل نشدن فرم نیست.

در نهایت بعد از تکمیل فرم؛ نیاز است تا حداقل ۷ الی ۱۰ روز صبر کنید تا گوگل فایل شما را بررسی و خطای Blocked by Play Protect برطرف گردد.

لطفا توجه داشته باشید در صورت تایید درخواست شما، هیچ‌گونه اطلاع‌رسانی صورت نخواهد گرفت و ایمیلی از جانب گوگل برای شما ارسال نخواهد شد. بنابراین بهتر است با روش زیر برنامه خود را تست کنید تا از عدم دریافت این خطا مطلع و برنامه را برای بازار مجدد در صف بررسی قرار دهید.

گوگل جلوی انتشار چه برنامه‌هایی را خواهد گرفت؟

این که توسعه‌دهندگان بدانند معیارهای گوگل برای تشخیص یک برنامه سالم یا خطرناک چیست به داشتن دید بهتر نسبت به دلایل رخ دادن Blocked By Play Protect کمک خواهد کرد. طبق آن‌چیزی که در این سند مطرح شده، گوگل برای آن‌که داشتن یک تجربه عالی را برای کاربران خود مطرح کند، نکاتی را برای امنیت بیشتر آن‌ها با حساسیت بالایی در مورد انتشار برنامه‌ها در نظر خواهد گرفت. لیست زیر را طبق اعلام گوگل می‌توان در دسته «ناخواسته‌ترین برنامه‌ها توسط کاربران» قرار می‌دهد:

- برنامه وعده محتوایی را به کاربر می‌دهد که با واقعیت آن برنامه مطابقت ندارد
- برنامه سعی می‌کند کاربران را برای نصب برنامه‌دیگر فریب دهد
- در مورد عملکردهای غیرمنتظره‌ای که ممکن است هنگام استفاده از برنامه رخ دهد هشداری به کاربر داده نمی‌شود
- حذف برنامه دشوار است
- اطلاعات خصوصی کاربران را بدون اطلاع آن‌ها جمع‌آوری کرده یا منتقل می‌کند
- به همراه آن نرم‌افزارهای دیگری هم روی دستگاه اندرویدی حضور پیدا می‌کنند که وجودشان برای کاربر فاش نمی‌شود.

دلایل بروز خطای Blocked By Play Protect

سرویس Play Protect روزانه تعداد زیادی از برنامه‌های موجود در دستگاه کاربران را اسکن می‌کند و در صورت وجود برنامه‌های مضر، به کاربران اعلان‌های لازم را می‌دهد.

- **درب پشتی و پنهان (Backdoor)**: کدی که امکان اجرای عملیات ناخواسته، مضر و کنترل از راه دور روی یک دستگاه را فراهم می‌کنند. به طور کلی، backdoor توصیفی است که چگونه یک عملیات بالقوه مضر روی یک دستگاه رخ می دهد. طبقه بندی بدافزارهای backdoor به نحوه عملکرد کد بستگی دارد. به عنوان مثال، اگر برنامه‌ای اجازه بارگذاری پویای کد را بدهد و کد بارگذاری شده به صورت پویا پیام‌های متنی را استخراج کند، به عنوان یک بدافزار مخفی طبقه بندی می‌شود. خطایی که کاربر در این حالت مشاهده می‌کند:
"This app can allow unauthorized access to your data or device."

- **تقلب صورتحساب (Billing Fraud)**: معنای کلی آن تحمیل هزینه‌های ناآگاهانه به کاربر است. مانند ارسال پیام کوتاه، برقراری تماس، یا هر نوع از خدماتی که بدون اطلاع کاربر فعال می‌شود. خطایی که کاربر در این حالت مشاهده می‌کند:

"؛This app can add unauthorized charges to your mobile bill by registering for recurring charges.

- **جاسوس تجاری (Commercial Spyware)**: مورد دیگر Commercial Spyware است که در این شرایط اطلاعات رفتاری کاربر بدون آگاهی او، توسط برنامه شناسایی و ذخیره شده و برای یک منبع خارجی ارسال می‌شود. خطایی که کاربر در این حالت مشاهده می‌کند:

"This app can spy on you by monitoring your location or your activity on this device."

- **خودداری از خدمات (Denial of Service or DoS)**: در این حالت درخواست‌های بسیاری برای یک سرویس‌دهنده ارسال می‌شود که به موجب آن، استفاده از آن سرویس را با اختلال مواجه می‌کند. در واقع حجم بالای این درخواست‌های ارسال شده، بدون اطلاع کاربر بوده که باعث می‌شود آن سرویس‌دهنده توانایی پاسخ‌گویی به کاربران واقعی را نداشته باشد. خطای مرتبط با پلی پروتکت که کاربر در این حالت مشاهده می‌کند:

"This app tries to attack other mobile and computer systems."

- **دانلود کننده دشمن (Hostile downloaders)**: برنامه به خودی خود مخرب نیست، ولی می‌تواند منبعی برای دانلود این دست از برنامه‌ها باشد که در این‌صورت باز هم مخرب شناسایی می‌شود. خطایی که کاربر در این حالت مشاهده می‌کند:

"This app can install potentially harmful apps without your permission."

تهدید غیر اندرویدی (Non-Android threat)

در این حالت، برنامه خطری برای کاربر با دستگاه اندرویدی ندارد، با این‌حال می‌تواند محتوایی داشته باشد که برای دستگاه‌های غیر اندرویدی تهدیدآمیز است و منجر به خطای پلی پروتکت می شود. به همین دلیل از نظر گوگل مخرب محسوب می‌شود. به عنوان مثال برنامه‌ی اندرویدی که شامل ویروسی برای سیستم عامل ویندوز است. در این شرایط خطری دستگاه اندرویدی کاربر را تهدید نمی‌کند ولی به محض اتصال به دستگاه ویندوزی، آن دستگاه آلوده خواهد شد. خطایی که کاربر در این حالت مشاهده می‌کند:

"This app can harm non-Android devices."

- **فیشینگ (Phishing)**: در این شرایط به نظر می‌آید برنامه از یک منبع معتبر و شناخته شده بوده و به صورت رسمی کار جمع‌آوری اطلاعات را انجام می‌دهد. این برنامه اطلاعات هویتی و رمزهای عبور کاربر را درخواست کرده و در صورتی‌که این اطلاعات برای یک منبع خارجی ارسال می‌شود. خطایی که کاربر در این حالت مشاهده می‌کند:

"This app is fake. It can steal your personal data, such as banking info and passwords."

- **سواستفاده از امتیاز (Elevated Privilege Abuse)**: برنامه‌ای با این خصوصیت، بسترهای امنیتی را هدف قرار می‌دهد و با متزلزل کردن این بستر شرایطی را فراهم می‌کند تا امکان دسترسی به هسته امنیتی وجود داشته باشد. خطایی که کاربر در این حالت مشاهده می‌کند:

"This app tries to bypass Android's security protections."

- **باج‌افزار (Ransomware)**: این قبیل برنامه‌ها کنترل دستگاه کاربر و یا داده‌های موجود در آن دستگاه را به‌دست می‌آورد و اقدام به تهدید کاربر و طلب باج می‌کند. خطایی که کاربر در این حالت مشاهده می‌کند:

"This app can disable your device or threaten to reveal personal information unless you pay money."

- **روت کردن (Rooting)**: این برنامه‌ها بدون اطلاع کاربر اقدام به روت کردن دستگاه می‌کنند. لازم به ذکر است روت کردن از مواردی است که کاربر ممکن است با اختیار خود انتخاب کند، با این‌حال برخی از برنامه‌ها این کار را بدون اطلاع وی انجام می‌دهند. ممکن است این برنامه‌ها روت کردن دستگاه را در راستای آن فعالیت‌هایی که پیش‌تر به آن اشاره شد انجام دهند و در نتیجه امنیت دستگاه اندرویدی کاربر را تهدید کنند. خطایی که کاربر در این حالت مشاهده می‌کند:

"This app tries to bypass Android's security protections."

- **اسپم (Spam)**: در این حالت، برنامه بدون اطلاع کاربر اقدام به ارسال پیام به مخاطبان ثبت شده در دستگاه او می‌کند و به نوعی از دستگاه کاربر به عنوان منبعی برای ارسال هرزنامه استفاده می‌کند. خطایی که کاربر در این حالت مشاهده می‌کند:

"This app can spam other people with unauthorized messages."

- **جاسوس‌افزار (Spyware)**: در این حالت، برنامه اطلاعات شخصی کاربر را بدون اطلاع و رضایت وی منتقل می‌کند. خطایی که کاربر در این حالت مشاهده می‌کند:

"This app tries to spy on your personal data, such as SMS messages, photos, audio recordings, or call history."

نکته: دسترسی‌های حساس‌تری که ممکن است توسط پلی پروتکت به عنوان جاسوس‌افزار شناخته شوند:

1. لیست مخاطبین و تماس
2. محتوا از ایمیل کاربر
3. لیست پیام کوتاه
4. تاریخچه مرورگر
5. اطلاعات از داده و فهرست سایر برنامه ها.

رفتارهایی که می‌توانند به عنوان جاسوسی از کاربر در نظر گرفته شوند، می‌توانند به عنوان جاسوس‌افزار نیز علامت گذاری شوند. به عنوان مثال ضبط صدا یا ضبط تماس‌های انجام شده یا سرقت داده‌های برنامه همگی از این موارد محسوب می‌شوند.

- **تروجان (Trojan)**: در این وضعیت، به نظر می‌رسد کارکرد برنامه مشابه با سایر برنامه‌هاست، در صورتی‌که در عمل فعالیت‌هایی در برنامه صورت می‌پذیرد که به منفعت کاربر لطمه وارد می‌کند. خطایی که کاربر در این حالت مشاهده می‌کند:

"This app is fake. It tries to take over your device or steal your data."

- **برنامه‌های غیر معمول (Uncommon):** برنامه‌های تازه منتشر شده و برنامه‌هایی که به ندرت مورد استفاده قرار می‌گیرند نیز ممکن است توسط گوگل به عنوان یک برنامهٔ مخرب شناسایی شوند. به این دلیل‌که اطلاعات کافی برای تضمین امنیت آن‌ها در گوگل وجود نداشته است. خطایی که کاربر در این حالت مشاهده می‌کند:

"Play Protect doesn't recognize this app's developer. Apps from unknown developers can sometimes be unsafe."

نرم افزارهای ناخواسته موبایل (Mobile Unwanted Software)

گوگل نرم افزار ناخواسته را به عنوان برنامه‌هایی تعریف می‌کند که بدافزار نیستند، اما برای اکوسیستم نرم افزارهای اندرویدی مضر هستند. نرم افزارهای ناخواسته موبایل دیگر برنامه‌ها را جعل می‌کنند یا حداقل یکی از موارد زیر را بدون رضایت کاربر جمع آوری می‌کند:

- شماره تلفن دستگاه
- آدرس ایمیل پیش‌فرض
- اطلاعات مربوط به برنامه های نصب شده
- اطلاعات مربوط به حساب‌های شخص ثالث

نرم‌افزارهای ناخواسته موبایل به صورت جدا از بدافزارها توسط پلی پروتکت ردیابی می شوند. می توانید دسته‌های نرم‌افزارهای ناخواسته که منجر به خطای پلی پروتکت می‌شوند را در ادامه مشاهده کنید

- **جمع‌آوری داده (Data Collection)**: این حالت برای برنامه‌هایی‌ست که داده‌ها را جمع‌آوری کنند و آن‌ها را بدون رضایت و آگاهی کاربر منتقل کنند. خطایی که کاربر در این حالت مشاهده می‌کند:
"This app can collect data that could be used to track you."

- **مهندسی اجتماعی (Social Engineering):** مهندسی اجتماعی به معنای نفوذ روانشناختی به افراد با هدف ارسال اطلاعات محرمانه آن‌هاست. خطایی که کاربر در این حالت مشاهده می‌کند:
"This app looks like another app and can trick you into exposing personal data, misusing your device, or installing other apps."

- **تبلیغات مخرب (Disruptive ads)**: در این حالت برنامه و خطای پلی پروتکت، تبلیغات را به صورت ناگهانی و غیرمنتظره به کاربر نمایش می‌دهد. خطایی که کاربر در این حالت مشاهده می‌کند:
“This app may display ads with unexpected behaviors (for example, outside the app environment, cannot be easily dismissed, or interfering with device functionality).”

- **استفاده غیرمجاز یا تقلید و شبیه‌سازی از عملکرد سیستم (Unauthorized Use or Imitation of System Functionality) :** برنامه‌ها یا تبلیغاتی که عملکرد سیستمی اندروید را تقلید یا با آن تداخل دارند، مانند اعلان‌ها و هشدارها. این نکته را در نظر بگیرید که اعلانات سطح سیستم فقط برای ویژگی‌های یکپارچه برنامه قابل استفاده است.

برای راهنمایی‌های بیشتر در رابطه با خطای پلی پروتکت می‌توانید با پشتیبانی بازار از طریق ثبت تیکت یا شماره تلفن ۰۲۱۹۱۰۰۹۷۹۸ در ارتباط باشید.

به مطالب ارائه شده چه امتیازی می‌دهید؟

محل نوشتن دیدگاه ...

اگر در مورد محتوا نظر یا پیشنهادی دارید لطفا برای ما بنویسید.

محل نوشتن دیدگاه ...

ارسال دیدگاه

زمان انتشار: ۱۴۰۰-۰۴-۰۸ ۱۹:۰۳

آخرین به‌روزرسانی: ۱۴۰۳-۱۰-۰۱ ۱۶:۰۲

فهرست مطالب