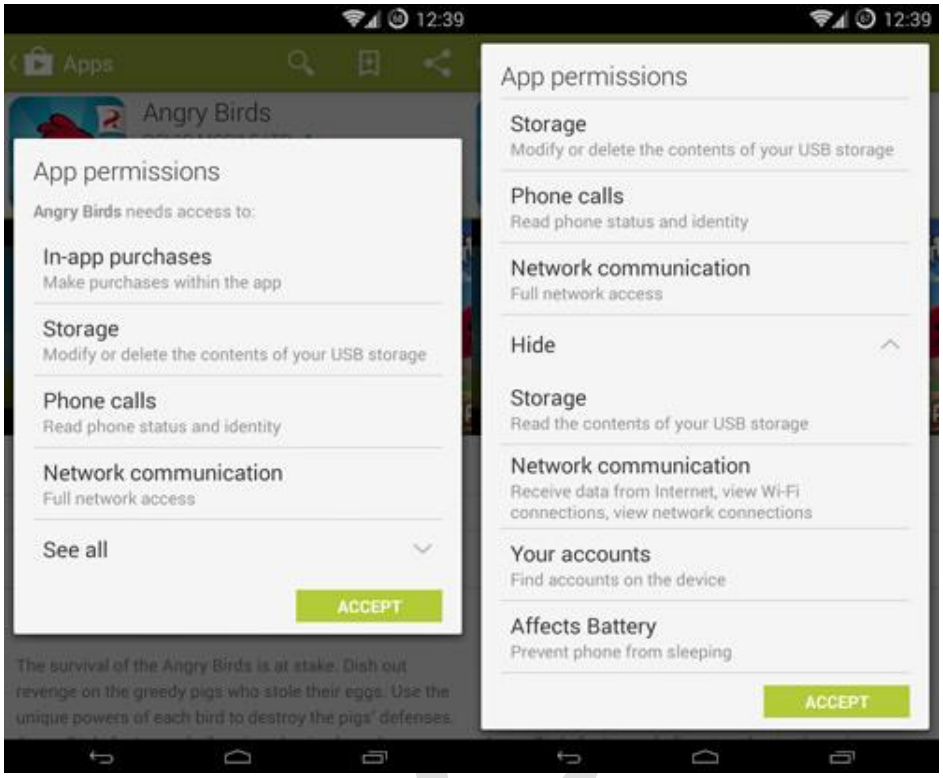
تحلیلی در زمینه مجوزهای برنامه‌های کاربردی سیستم‌عامل اندروید

امروزه با توجه به تولید انبوه برنامه‌های کاربردی اندرویدی و ارائه آن‌ها در بازارهای ایرانی و خارجی و همچنین دانش اندک بیشتر کاربران سیستم‌عامل اندروید، باید در مورد خطرات احتمالی آن دست از برنامه‌هایی که تهدیداتی را برای کاربران دستگاه‌های اندرویدی ایجاد می‌کنند اطلاع‌رسانی شود. بسیاری از برنامه‌های کاربردی چه ایرانی و چه خارجی با دریافت یکسری مجوزهای حساس با استفاده از مهندسی اجتماعی و یا عدم آگاهی کافی کاربران اقدام به سرقت اطلاعات کاربران می‌کنند. ولی سؤالی که باید پرسیده شود این است که آیا تابه‌حال مجوزهای درخواستی برنامه کاربردی اندرویدی شما قبل از نصب را مطالعه کرده‌اید؟ تعداد افرادی که این مجوزها را مطالعه می‌کنند انگشت‌شمار هستند و بیشتر افراد برخوردی عادی و بی‌تفاوت به این مجوزها دارند. از عدم آگاهی و نیز بی‌توجهی بیشتر کاربران، توسعه‌دهندگان برنامه‌های کاربردی مجوزهایی را از کاربران می‌خواهند که راه را برای نفوذ به دستگاه‌های اندرویدی باز می‌کند. هدف از این گزارش آگاه‌سازی کاربران در مورد مجوزهایی است که برنامه‌های کاربردی اندرویدی درخواست می‌کنند.

در ابتدا باید عنوان کرد که مجوزهای اندروید درخواست نیستند بلکه یک اعلان یا اطلاع‌رسانی را به کاربران اعلام می‌دارند. هنگامی‌که یک برنامه کاربردی را از Play Store دریافت و نصب می‌کنیم یک پنجره پاپ آپ ظاهر می‌شود که تمام مجوزهای درخواستی برنامه کاربردی موردنظر را به نمایش می‌گذارد که این مجوزها می‌توانند دسترسی به حافظه گوشی موردنظر، تماس‌های تلفنی، ارتباطات شبکه و غیره را داشته باشند.



شاید رد کردن یا تفویض مجوزهای درخواستی برنامه کاربردی در حال نصب ساده‌ترین کاری باشد که یک کاربر می‌تواند انجام دهد اما نکته مهم این است که تا چه اندازه می‌توان تفاوت بین حفاظت و تأمین امنیت داده کاربر و نیز در اختیار قرار دادن تمام دارایی‌های شخص در دست توسعه‌دهنده برنامه کاربردی را درک نمود.

بیشتر شرکت‌های اینترنتی از متدهای عمومی مشابهی برای آگاه‌سازی کاربران در خصوص داده‌هایی که قرار است مورداستفاده قرار گیرند بهره می‌برند. در سیستم‌عامل اندروید یک ارتباط سه سویه بین **کاربر**، **گوگل** (طراح و ارائه‌دهنده سیستم‌عامل اندروید) و **توسعه‌دهندگان** برنامه کاربردی شخص سوم وجود دارد. گوگل درواقع ارتباط بین کاربر و توسعه‌دهندگان شخص سوم را با استفاده از مجموعه‌ای از مجوزها برای هر برنامه کاربردی دانلود شده توسط کاربر، مدیریت می‌کند. مجوزها درواقع نیازمندی‌های توسعه‌دهندگان را برای چگونگی تعامل برنامه کاربردی تولیدشده با دستگاه کاربر مشخص کرده و دسترسی به نوع اطلاعات درخواستی برنامه کاربردی را نیز تعیین خواهد کرد.

در اکوسیستم اندروید بیشترین فشار بر روی توسعه‌دهندگان است تا مجوزهایی که به کاربر نشان داده می‌شوند، نحوه کار برنامه کاربردی را به‌درستی انتخاب و به نمایش بگذارند. پس‌ازاینکه **توسعه‌دهنده برنامه کاربردی یک برنامه را ایجاد کرد، مجوزهای صحیح را به‌درستی انتخاب نمود** و **لیستی از کاربران هدفی که درنهایت با این مجوزها موافقت نموده‌اند** را تهیه کرد، گوگل برنامه کاربردی تولیدی را به‌منظور شناسایی بدافزار و تشخیص کدهای مخرب مورد ارزیابی قرار خواهد داد. محدوده مجوزها برای تعامل برنامه کاربردی

از اجازه دسترسی به بخش ویژه‌ای از سخت‌افزار دستگاه (به‌عنوان‌مثال فلش دوربین عکاسی) آغاز می‌شود و تا دسترسی به لیست مخاطبان کاربر ادامه می‌یابد. کاربر نیز باید با تمام مجوزهای لیست شده قبل از نصب برنامه کاربردی موافقت نماید.

اصول مجوزهای برنامه‌های کاربردی گوگل

مستندسازی مجوزها آن‌هم با وجود تنوع زیاد مجوزها و نیازمندی‌های متفاوت برنامه‌های کاربردی از کاربران بسیار سخت است. در این بخش گزارشی از بررسی مجوزهای برنامه‌های موجود در فروشگاه Google Play با تمرکز ویژه روی مجوزهایی که به‌صورت بالقوه به برنامه کاربردی این اجازه را می‌دهند تا اطلاعات شخصی کاربر را جمع‌آوری و یا به اشتراک بگذارند ارائه شده است.

درمجموع با بررسی ۱۰۴۱۳۳۶ برنامه کاربردی در این آزمایش باید عنوان کرد که تنها ۲۳۵ مجوز انحصاری و خاص وجود داشته است. بیشتر برنامه‌های کاربردی مجوزهای زیادی را طلب می‌کنند و بیشترین تعداد مجوزهای درخواستی از برنامه‌های کاربردی این آزمون تعداد ۱۲۷ مجوز بوده است که برای یک برنامه کاربردی مقدار بسیار زیادی است. برنامه‌های کاربردی دیگری هم هستند که تعداد انگشت‌شماری مجوز درخواست می‌کنند که میانگین مجوزهای درخواستی از یک برنامه کاربردی تنها ۵ مجوز بوده است. در این گزارش تحلیلی باید اشاره کرد که ۱۰۰۰۰۰ برنامه نیز مجوزی را درخواست نکرده‌اند.

بیشترین مجوزهای برنامه‌های کاربردی در فروشگاه Google Play				
مجوز	**کاری که مجوز انجام می‌دهد "به برنامه کاربردی اجازه می‌دهد تا ..."**	**تعداد برنامه‌های کاربردی**	**٪ از برنامه‌های کاربردی**	**مجوز سخت‌افزاری یا اطلاعات کاربر**
دسترسی کامل به شبکه (Full network access)	... یک درگاه شبکه ایجاد کرده و از پروتکل‌های معمول شبکه استفاده می‌کند. مرورگر و دیگر برنامه‌های کاربردی داده را از طریق اینترنت ارسال می‌کنند که این بدان معنا است که مجوز نیازی به ارسال داده از طریق اینترنت را نباید داشته باشد.	۸۵۵۸۷۳	٪۸۳	سخت‌افزار
مشاهده ارتباطات شبکه (View network connections)	... مشاهده اطلاعات درباره ارتباطات شبکه، به‌عنوان‌مثال تشخیص اینکه کدام شبکه وجود دارد و متصل است.	۷۱۴۶۰۷	٪۶۹	سخت‌افزار
آزمون دسترسی به حافظه حفاظت‌شده (Test access to protected storage)	... آزمون مجوز مربوط به حافظه USB که بر روی دستگاه‌های آینده قابل‌دسترس خواهند بود. به برنامه کاربردی اجازه می‌دهد تا مجوز را برای SD card آزمایش نماید.	۵۶۲۴۴۲	٪۵۴	سخت‌افزار
تنظیم یا حذف محتوای موجود بر روی حافظه USB	... نوشتن بر روی حافظه USB. به برنامه کاربردی اجازه نوشتن بر روی SD card را می‌دهد.	۵۵۹۹۴۱	٪۵۴	اطلاعات کاربر

(Modify or delete the contents of your USB storage)				
خواندن وضعیت تلفن و هویت (Read phone status and identity)	... دسترسی به ویژگی‌های تلفن. این مجوز به برنامه کاربردی اجازه می‌دهد تا شماره‌های تلفن و ID را به هنگام برقراری تماس تشخیص دهد.	۳۶۱۶۱۶	٪۳۵	اطلاعات کاربر
جلوگیری از به خواب رفتن گوشی (Prevent device from sleeping)	... ممانعت از به خواب رفتن گوشی. به برنامه کاربردی اجازه می‌دهد تا مانع به خواب رفتن گوشی شود.	۲۷۹۷۷۵	٪۲۷	سخت‌افزار
موقعیت مکانی دقیق(مبتنی بر GPS و شبکه) (Precise location(GPS and network-based)	... دریافت موقعیت مکانی دقیق با استفاده از سیستم موقعیت‌یاب جهانی (GPS) یا موقعیت مکانی دکل‌های مخابراتی و Wi-Fi. این سرویس‌های موقعیت مکانی باید برای دستگاه موردنظر فعال و قابل‌دسترس باشند تا برنامه کاربردی قابلیت استفاده از آن را داشته باشد. برنامه‌های کاربردی توانایی تشخیص موقعیت مکانی شما را با استفاده از این مجوز دارند و به سبب آن مصرف انرژی بیشتری را برای دستگاه به همراه خواهند داشت.	۲۴۶۷۵۰	٪۲۴	اطلاعات کاربر
مشاهده ارتباطات بی‌سیم Wi-Fi (View Wi-Fi connections)	... مشاهده اطلاعاتی درباره شبکه‌های Wi-Fi، ازجمله تشخیص فعال بودن Wi-Fi و اسامی دستگاه‌های Wi-Fi متصل شده.	۲۳۵۰۹۳	٪۲۳	اطلاعات کاربر
کنترل لرزاننده (Control vibration)	... کنترل‌کننده لرزاننده	۲۲۰۵۹۴	٪۲۱	سخت‌افزار
موقعیت تقریبی(مبتنی بر شبکه) (Approximate location (network-based)	... دریافت موقعیت مکانی تقریبی. این موقعیت مکانی از طریق سرویس‌های موقعیت مکانی به‌ویژه دکل‌های سلولی و Wi-Fi به‌دست می‌آیند. این سرویس‌های موقعیت مکانی باید برای دستگاه موردنظر فعال و قابل‌دسترس باشند تا برنامه کاربردی قابلیت استفاده از آن را داشته باشد. برنامه‌های کاربردی توانایی تشخیص تقریبی موقعیت مکانی شما را با استفاده از این مجوز خواهند داشت.	۲۱۶۷۷۰	٪۲۱	اطلاعات کاربر

از مجموع ۲۳۵ مجوز که در این گزارش تحلیلی شناسایی شده‌اند تنها ۱۰ مجوز توسط ۲۰٪ برنامه‌های کاربردی موجود در Google Play مورداستفاده قرارگرفته است و تعداد زیادی از مجوزها تنها توسط بخش اندکی از برنامه‌های کاربردی درخواست شده‌اند. اگر بخواهیم به‌صورت آماری نگاه کنیم تعداد ۱۰۰۰ برنامه از مجموع ۱۰۴۱۳۳۶ که ۰.۰۹٪ از تعداد کل برنامه‌های کاربردی مورد تحلیل را شامل می‌شوند، مقدار ۱۴۷

مجوز از مجموع ۲۳۵ مجوز را درخواست کرده‌اند که با توجه به کل برنامه‌های مورد ارزیابی، مقدار زیادی از مجوزها را پوشش می‌دهند. البته باید این نکته را نیز اضافه نمود که مجموع مجوزهای درخواستی از یک برنامه کاربردی به‌صراحت نمی‌تواند مشخص کند برنامه مورد نظر توانایی دسترسی به چه مقدار از اطلاعات کاربر را خواهد داشت. تناقضی که وجود دارد این است که یک برنامه کاربردی تنها با **یک مجوز** توانایی دسترسی به‌تمامی اطلاعات کاربر را می‌تواند داشته باشد درحالی‌که یک برنامه کاربردی با تعداد مجوزهای درخواستی فراوان تنها قابلیت تعامل با اجزای سخت‌افزاری دستگاه موردنظر را خواهد داشت! تحلیل ذکرشده به بررسی عمیق‌تر بر روی برنامه کاربردی به‌ویژه نوع مجوزهای درخواستی آن‌ها در فروشگاه Google Play می‌پردازد.

به‌طور ویژه مجوزهایی که نسبت به سایر مجوزها شایع‌تر هستند به دو دسته تقسیم می‌شوند:

- مجوزهایی که به برنامه کاربردی این اجازه را می‌دهند تا به اطلاعات کاربر دسترسی داشته باشند.
- مجوزهایی که به برنامه کاربردی اجازه می‌دهند تا به‌صورت مستقیم با دستگاه تعامل داشته باشند.

توجه

تعریف "اطلاعات کاربر" یک تعریف عام از اطلاعات کاربر است. مجوزهایی که جهت دریافت "اطلاعات کاربر" صادر می‌شوند، فرض شده‌اند که هر نوع اطلاعات مربوط به کاربر را پوشش خواهند داد. به همین ترتیب مجوزهای صادرشده مبتنی بر دسترسی به سخت‌افزار دستگاه نیز الزاماً بخش مشخصی از سخت‌افزار نخواهد بود.

مجوزهایی که سخت‌افزار دستگاه را تحت کنترل قرار می‌دهند

از ۲۳۵ مجوز انحصاری جمع‌آوری‌شده در این تحلیل، ۱۶۵ نوع از آن‌ها به برنامه کاربردی اجازه می‌دهند تا با اجزای سخت‌افزاری یک دستگاه تعامل داشته باشند و به برنامه اجازه دسترسی دیگری ازجمله اطلاعات کاربر را نخواهد داد.

به‌عنوان‌مثال دو نمونه از عمومی‌ترین مجوزها به برنامه کاربردی اجازه اتصال به اینترنت را می‌دهند. مجوز "دسترسی کامل به شبکه" (که توسط ۸۳٪ برنامه‌های کاربردی مورداستفاده قرار می‌گیرند.) به برنامه کاربردی این اجازه را می‌دهد تا با هر شبکه‌ای که دستگاه به آن متصل است ارتباط برقرار نماید. درحالی‌که مجوز "مشاهده ارتباطات شبکه" (که توسط ۶۹٪ برنامه‌های کاربردی مورداستفاده قرار می‌گیرند.) به برنامه کاربردی این اجازه را می‌دهد تا هر شبکه‌ای که دستگاه به آن دسترسی دارد را ببیند. هر برنامه کاربردی که درخواست دسترسی به اینترنت را داشته باشد، به‌منظور افزایش قابلیت‌های خود ممکن است به هردو مجوز

"اطلاعات کاربر" و "مجوز سخت‌افزار" نیاز داشته باشد. درحالی‌که این دو مجوز به‌شدت فراگیر هستند اما اجازه دسترسی مستقیم به اطلاعات کاربر را به برنامه کاربردی نمی‌دهند.

نمونه‌هایی از کارکردهای این دست از مجوزها:

کنترل چراغ‌قوه – این مجوز به برنامه کاربردی این اجازه را می‌دهد تا با چراغ(فلش) موجود در گوشی هوشمند و یا رایانک مالشی تعامل داشته باشد. عموماً این چراغ مربوط به دوربین عکاسی است اما یک برنامه کاربردی توانایی استفاده از چراغ دوربین با قابلیت روشن و یا خاموش نگاه‌داشتن ممتد برای ایجاد یک "چراغ‌قوه" را خواهد داشت.

تنظیمات تصاویر زمینه – این مجوز به یک برنامه کاربردی این اجازه را خواهد داد تا یک تصویر را در پس‌زمینه صفحه‌نمایش خانگی یک دستگاه تنظیم نماید (معمولاً در دستگاه‌های مبتنی بر سیستم‌عامل اندروید آن را "تصویر زمینه" نیز می‌نامند).

کنترل لرزاننده – این مجوز به یک برنامه کاربردی اجازه کنترل لرزاننده که در بیشتر گوشی‌های هوشمند وجود دارند را خواهد داد.

این نوع از مجوزها خیلی هم ساده و سطحی نیستند. اگر از این نوع از مجوزها به‌درستی استفاده نشوند (و یا به‌صورت مخرب استفاده شوند) یک برنامه کاربردی با یکی از این مجوزها می‌تواند به‌صورت بالقوه برای دستگاه کاربر خرابی و تهدید ایجاد نماید؛ اما این نوع از مجوزها به‌خودی‌خود به یک برنامه کاربردی اجازه دسترسی به اطلاعات کاربر را نمی‌دهند و باید کاربر مهر تائید را به آن برنامه کاربردی داده باشد.

مجوزهایی که دسترسی به اطلاعات کاربر را می‌دهند

دومین دسته‌بندی از مجوزها به برنامه کاربردی این اجازه را خواهند داد تا به انواع اطلاعات کاربر دسترسی داشته باشد. این دسته از مجوزها عموماً نسبت به دسته قبلی کمتر تفویض می‌شوند. درواقع از مجموع ۲۳۵ مجوز مشخص‌شده در این آزمون، ۷۰ مجوز به‌صورت بالقوه دسترسی به اطلاعات کاربر را ممکن خواهند ساخت.

نمونه‌هایی از این نوع مجوزها می‌تواند مجوزهایی باشند که به برنامه کاربردی اجازه می‌دهند تا تصاویر موجود در کتابخانه تصاویر کاربر را تغییر و یا حذف نماید. نمونه دیگر از این نوع مجوزها می‌تواند خواندن لیست مخاطبان کاربر نیز باشد.

بیشترین مجوزهای برنامه‌های کاربردی که توانایی دسترسی به اطلاعات کاربر را دارند			
مجوز	کاری که مجوز انجام می‌دهد "به برنامه کاربردی اجازه می‌دهد تا ..."	تعداد از برنامه‌های کاربردی	٪ از برنامه‌های کاربردی

تغییر یا حذف محتوا از حافظه USB (Modify or delete the contents of your USB storage)	... نوشتن روی حافظه USB. به برنامه کاربردی اجازه نوشتن روی SD card را می‌دهد.	۵۵۹۹۴۱	٪۵۴
خواندن وضعیت و هویت تلفن (Read phone status and identity)	... دسترسی به قابلیت‌های تلفن دستگاه. این مجوز به برنامه کاربردی اجازه تشخیص شماره تلفن و ID دستگاه را به هنگام برقراری تماس خواهد داد.	۳۶۱۶۱۶	٪۳۵
موقعیت مکانی دقیق(مبتنی بر GPS و شبکه) (Precise location (GPS and network-based))	دریافت موقعیت مکانی دقیق با استفاده از سیستم موقعیت‌یاب جهانی (GPS) یا موقعیت مکانی دکل‌های مخابراتی و Wi-Fi. این سرویس‌های موقعیت مکانی باید برای دستگاه موردنظر فعال و قابل‌دسترس باشند تا برنامه کاربردی قابلیت استفاده از آن را داشته باشد. برنامه‌های کاربردی توانایی تشخیص موقعیت مکانی شما را با استفاده از این مجوز خواهند یافت و به سبب آن مصرف انرژی بیشتری را برای دستگاه به همراه خواهند داشت.	۲۴۶۷۵۰	٪۲۴
مشاهده ارتباطات بی‌سیم Wi-Fi (View Wi-Fi connections)	... مشاهده اطلاعاتی درباره شبکه‌ها Wi-Fi، ازجمله تشخیص فعال بودن Wi-Fi و اسامی دستگاه‌های Wi-Fi متصل شده.	۲۳۵۰۹۳	٪۲۳
موقعیت تقریبی(مبتنی بر شبکه) (Approximate location (network-based))	... دریافت موقعیت مکانی تقریبی. این موقعیت مکانی از طریق سرویس‌های موقعیت مکانی به‌ویژه دکل‌های سلولی و Wi-Fi به‌دست می‌آیند. این سرویس‌های موقعیت مکانی باید برای دستگاه مورد نظر فعال و قابل‌دسترس باشند تا برنامه کاربردی قابلیت استفاده از آن را داشته باشد. برنامه‌های کاربردی توانایی تشخیص تقریبی موقعیت مکانی شما را با استفاده از این مجوز خواهند داشت.	۲۱۶۷۷۰	٪۲۱
پیدا کردن حساب‌های کاربری روی دستگاه (Find accounts on the device)	... دریافت لیست حساب‌های کاربری شناخته‌شده برای دستگاه که می‌تواند شامل هر حساب کاربری ایجادشده توسط برنامه کاربردی نصب‌شده روی دستگاه را پوشش دهد. به برنامه کاربردی اجازه می‌دهد تا لیست حساب‌های کاربری شناخته‌شده در دستگاه را دریافت نماید.	۱۶۲۹۲۵	٪۱۶
گرفتن عکس و فیلم (Take pictures and videos)	... گرفتن عکس و فیلم از طریق دوربین دستگاه. این مجوز به برنامه کاربردی اجازه خواهد داد تا با استفاده از دوربین تعبیه‌شده در دستگاه بدون گرفتن تائید از کاربر اقدام به گرفتن عکس و فیلم نماید.	۱۲۴۷۳۳	٪۱۲
برقراری تماس مستقیم با شماره‌های تلفن موجود در دستگاه (Directly call phone numbers)	... برقراری تماس با شماره‌های تلفن دستگاه، ازجمله شماره‌های ضروری، بدون مداخله کاربر. برنامه‌های کاربردی مخرب می‌توانند تماس‌های غیرضروری و غیرقانونی را با سرویس‌های اورژانس برقرار نمایند.	۸۴۲۹۰	٪۸
خواندن لیست مخاطبان (Read your contacts)	... خواندن داده‌های مربوط به لیست مخاطبان ذخیره‌شده در رایانک مالشی شما که می‌تواند شامل مخاطبانی که دفعات زیادی اقدام به برقراری تماس، ارسال ایمیل کرده‌اید. این مجوز به برنامه‌های کاربردی اجازه خواهند داد تا داده‌های لیست مخاطبان شما را ذخیره کنند، یک برنامه مخرب می‌تواند بدون آگاهی شما لیست مخاطبان را به اشتراک بگذارد.	۶۴۳۷۷	٪۶

خواندن لاگ‌های تماس (Read call log)	... خواندن لاگ تماس که می‌تواند درباره داده‌های تماس ورودی و خروجی باشد. این مجوز به برنامه‌های کاربردی اجازه خواهند داد تا داده‌های لاگ تماس را ذخیره کنند و برنامه‌های کاربردی مخرب می‌توانند این داده‌ها را به اشتراک بگذارند.	۴۲۷۹۷	٪۴

اگر بخواهیم به‌صورت موردی بررسی کنیم، مجوزی مثل مشاهده ارتباطات بی‌سیم ممکن است اطلاعات بسیار کمی را برای برنامه کاربردی افشا نماید اما یک برنامه کاربردی می‌تواند شبکه‌های بی‌سیم در دسترس را مشاهده نموده و اطلاعات‌پایه در مورد آن‌ها را جمع‌آوری نماید. در مورد نوع اطلاعات جمع‌آوری‌شده و منظور و هدف جمع‌آوری این دست از اطلاعات باید مشخص نمود که برنامه موردنظر به چه منظوری و با چه نیتی این اطلاعات را جمع‌آوری نموده است تا مشخص شود چه نوع اطلاعاتی ازنظر کاربر حساس و ضروری هستند؛ بنابراین هرگونه اطلاعات از کاربر می‌تواند به‌صورت بالقوه حساس باشد و مورد تحلیل قرار گیرد.

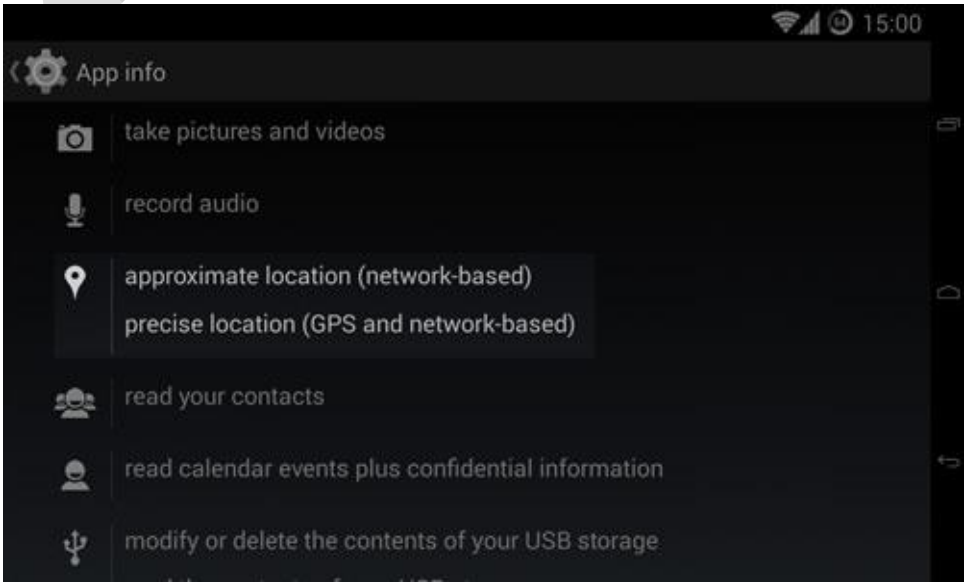
۵ مجوزی که باید نسبت به آن‌ها محتاط‌تر باشید

تعداد اندکی از مجوزها هستند که باید در خصوص آن‌ها احتیاط لازم را مبذول نمایید. البته نه به خاطر اینکه این نوع از مجوزها خطرناک هستند، بلکه به این دلیل که تفویض این نوع مجوزها ممکن است پیامدهای وسیعی را برای کاربر به همراه خواهد داشت، البته این پیامد زمانی حاصل خواهد شد که داده‌های کاربر در دست شخص نادرستی قرار گیرند.

۱. موقعیت مکانی

دو نمونه از مجوزهای موقعیت مکانی وجود دارند که برنامه‌های کاربردی اندرویدی به آن نیازمند هستند.

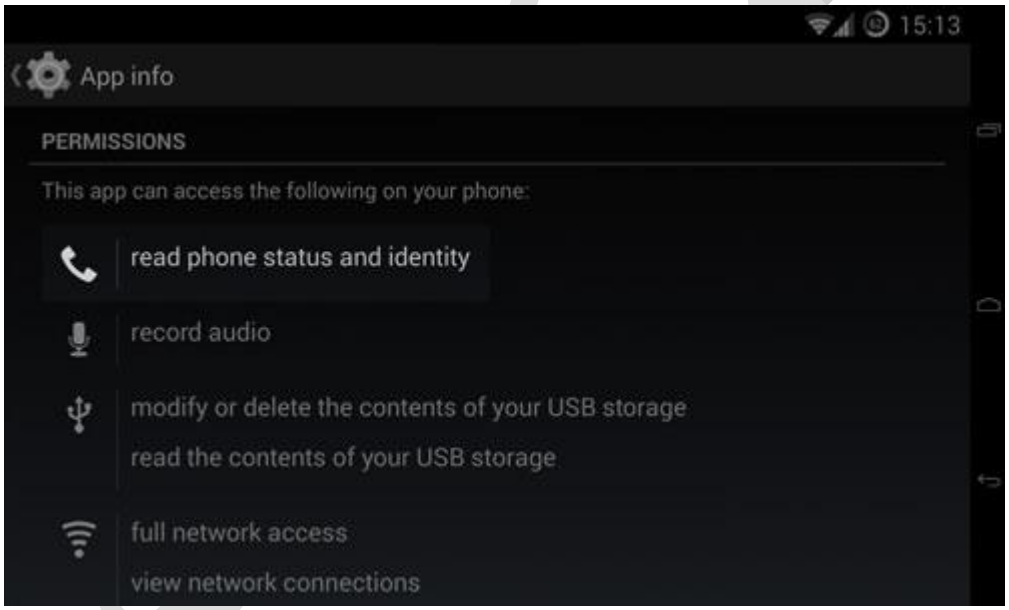
- موقعیت مکانی تقریبی (مبتنی بر شبکه)
- موقعیت مکانی دقیق (مبتنی بر GPS و شبکه)



سؤالی که وجود دارد این است که برنامه کاربردی برای چه منظوری نیازمند موقعیت مکانی دقیق شما است؟ به‌عنوان‌مثال برنامه کاربردی موقعیت‌یاب Waze برای اجرا نیازمند چنین اطلاعاتی خواهد بود. مهم‌تر این‌که برخی از برنامه‌های کاربردی هدفشان ارسال آگهی‌های بازرگانی بر اساس موقعیت مکانی کاربران است که این دست از برنامه‌ها نیز خواهان دسترسی به اطلاعات مکانی کاربر خواهند بود. البته این دست از برنامه‌های کاربردی عموماً رایگان هستند که در زمان اجرا آگهی‌های بازرگانی را نیز بر اساس موقعیت مکانی کاربر به نمایش می‌گذارند.

۲. وضعیت گوشی و هویت آن

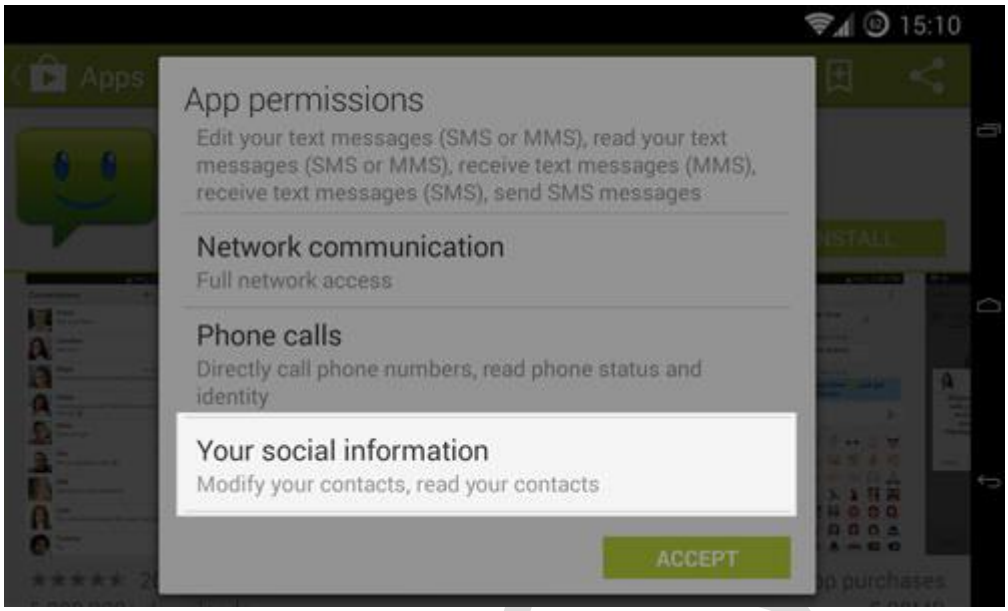
این نوع مجوز مشکل‌ساز خواهد بود زیرا تمامی اطلاعات مربوط به نیازمندی‌های یک تماس ورودی به گوشی همراه ازجمله شماره IMEI دستگاه موردنظر را به برنامه کاربردی خواهد داد.



این نوع مجوز ممکن است به‌صورت بالقوه برای مقاصد خرابکارانه مورداستفاده قرار بگیرد بنابراین به هنگام درخواست برنامه کاربردی برای دریافت این مجوز محتاط‌تر عمل کنید. اگر برنامه‌ای بدون دلیل منطقی درخواست چنین مجوزی را نمود به بررسی مجوز با توجه به کارایی آن برنامه اقدام نمایید.

۳. خواندن و تنظیم لیست مخاطبان شما

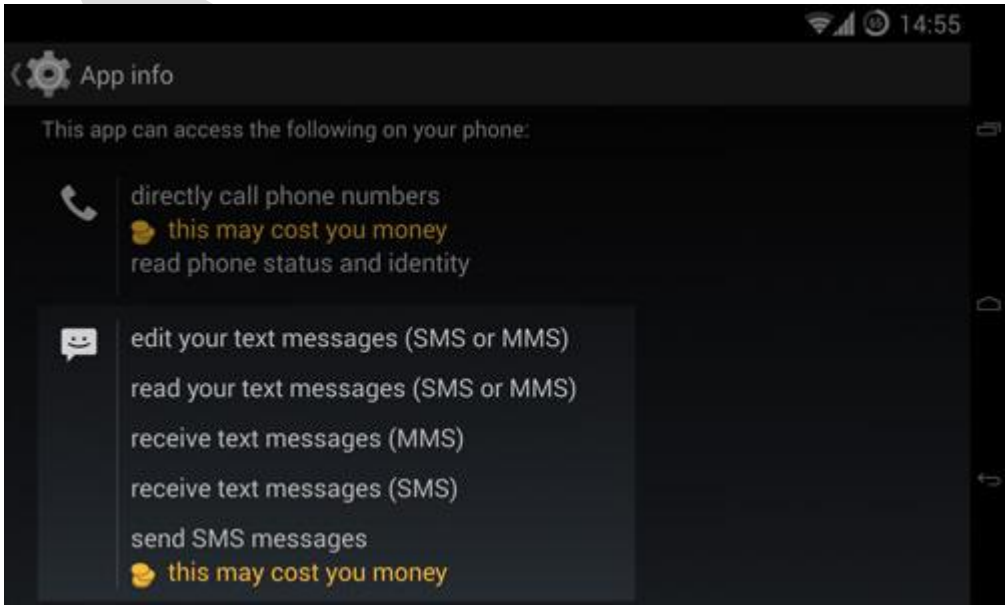
این نوع از مجوزهایی که برنامه کاربردی نیازمند دسترسی به خواندن و تنظیم مخاطبان کاربر هستند می‌تواند مشکل‌ساز شود، درواقع مجوز تنظیم مخاطبان زمانی خطرناک خواهد بود که برنامه کاربردی مجوز خواندن تمامی اطلاعات موجود روی گوشی شما را دریافت نماید.



برنامه‌های کاربردی مدیریت SMS، برنامه‌های کاربردی مدیریت مخاطبان، برنامه کاربردی که جایگزین شماره‌گیر گوشی می‌شوند و حتی برخی از برنامه‌های کاربردی اجتماعی نیز نیازمند چنین مجوزهایی خواهند بود ولی نکته‌ای که وجود دارد این است که برنامه‌های کاربردی که جنبه‌های اجتماعی ندارند لزومی به تفویض چنین مجوزهایی را نخواهند داشت.

۴. مجوزهای مربوط به SMS و MMS

این نوع از مجوزها می‌توانند به‌صورت بالقوه هزینه‌هایی را برای کاربر ایجاد نمایند، اگر برنامه کاربردی مخربی ازاین‌گونه مجوزها استفاده کند هزینه‌هایی را به‌وسیله SMS های قانونی و یا اعمال یکسری هزینه‌های اضافی به ازای هر SMS و MMS ارسالی برای کاربر ایجاد خواهد کرد.

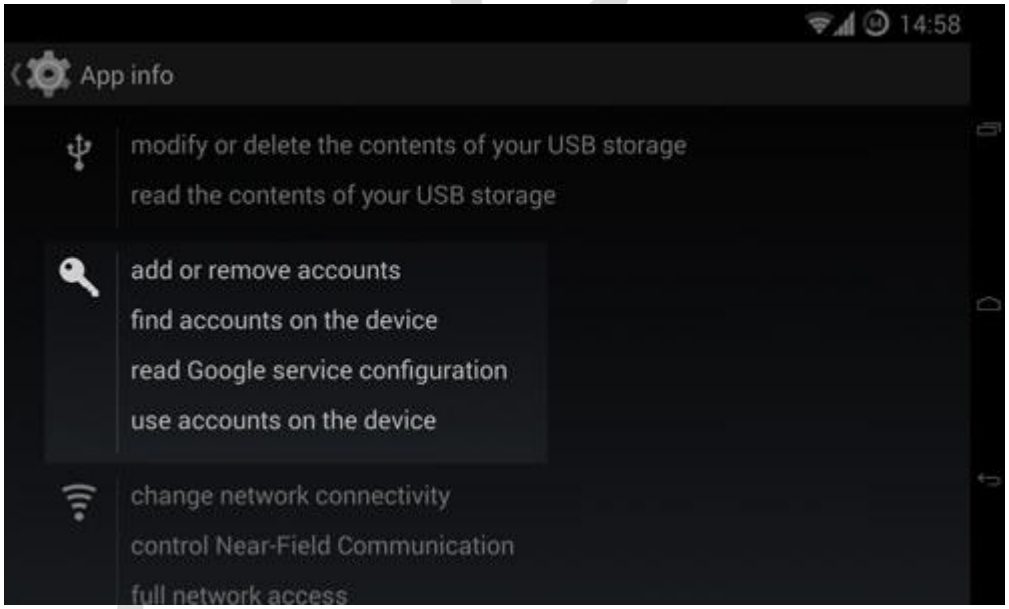


مجوزهای **خواندن پیام‌های متنی** و **دریافت پیام‌های متنی** توانایی نفوذ به حریم خصوصی شما را خواهند داشت اگر دلیل خاصی برای تفویض این نوع از مجوزها به برنامه کاربردی خود ندیدید از دادن این مجوزها جدا خودداری کنید.

۵. مجوزهای مربوط به حساب‌های کاربری

پیدا کردن حساب‌های کاربری بر روی دستگاه به برنامه کاربردی این امکان را می‌دهد تا از طریق مدیریت حساب‌های کاربری که سیستم‌عامل اندروید در خود جای‌داده است به بررسی حساب‌های کاربری ازجمله سرویس‌های google، Facebook و غیره نماید.

استفاده از حساب‌های کاربری روی دستگاه اندرویدی به برنامه کاربردی اجازه می‌دهد تا برای استفاده از حساب کاربری درخواست مجوز نماید. هنگامی‌که مجوز موردنیاز داده شد برنامه کاربردی موردنظر دیگر درخواست مجدد مجوز نخواهد کرد. نگرانی زمانی وجود خواهد داشت که برنامه کاربردی مخرب بدون هیچ‌گونه نشان و رد پایی به کار خود ادامه می‌دهد و به‌صورت مخفیانه از حساب کاربری شما استفاده خواهد کرد.



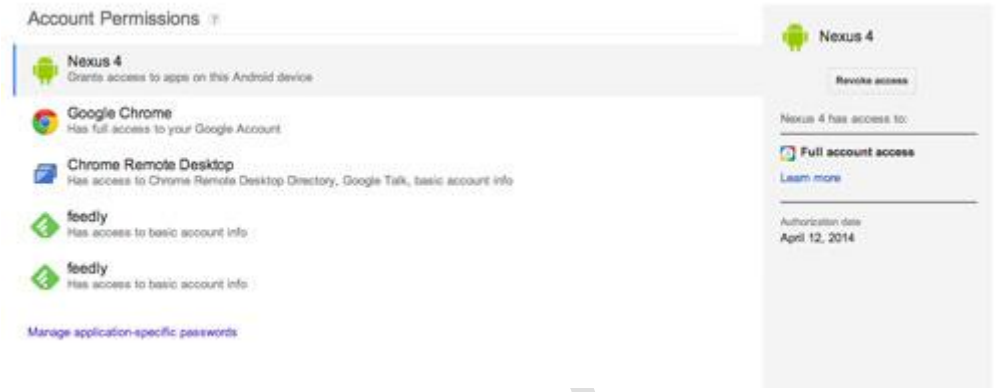
راهکارهای ایمنی

- بهترین راه برای ایمن ماندن رد درخواست برنامه کاربردی متقاضی مجوز مشکل ساز نیست، در عوض باید به نوع کارکرد برنامه کاربردی نگاه کرد و علت درخواست مجوز با توجه به کاری که آن برنامه انجام می‌دهد را بررسی نمود تا در صورت صحیح بودن علت درخواست مجوز موردنیاز به آن داده شود.
- شما می‌توانید با ارسال یک ایمیل به توسعه‌دهنده برنامه کاربردی موردنظر درباره مجوزهای درخواستی سؤال کنید. اگر پاسخ توسعه‌دهنده راضی‌کننده نبود یا پاسخی را در کل از توسعه‌دهنده دریافت نکردید باید به برنامه کاربردی مجوز موردنیاز را ندهید.

- اگر در مورد امنیت برنامه موردنظر اطمینان لازم را ندارید، شما باید از نقطه نظرات کاربران در خصوص استفاده از برنامه کاربردی استفاده کنید. (با بررسی فروم‌ها و فروشگاه‌های برنامه‌های کاربردی به نظرات کاربران توجه ویژه داشته باشید.)

مدیریت مجوزهای برنامه کاربردی

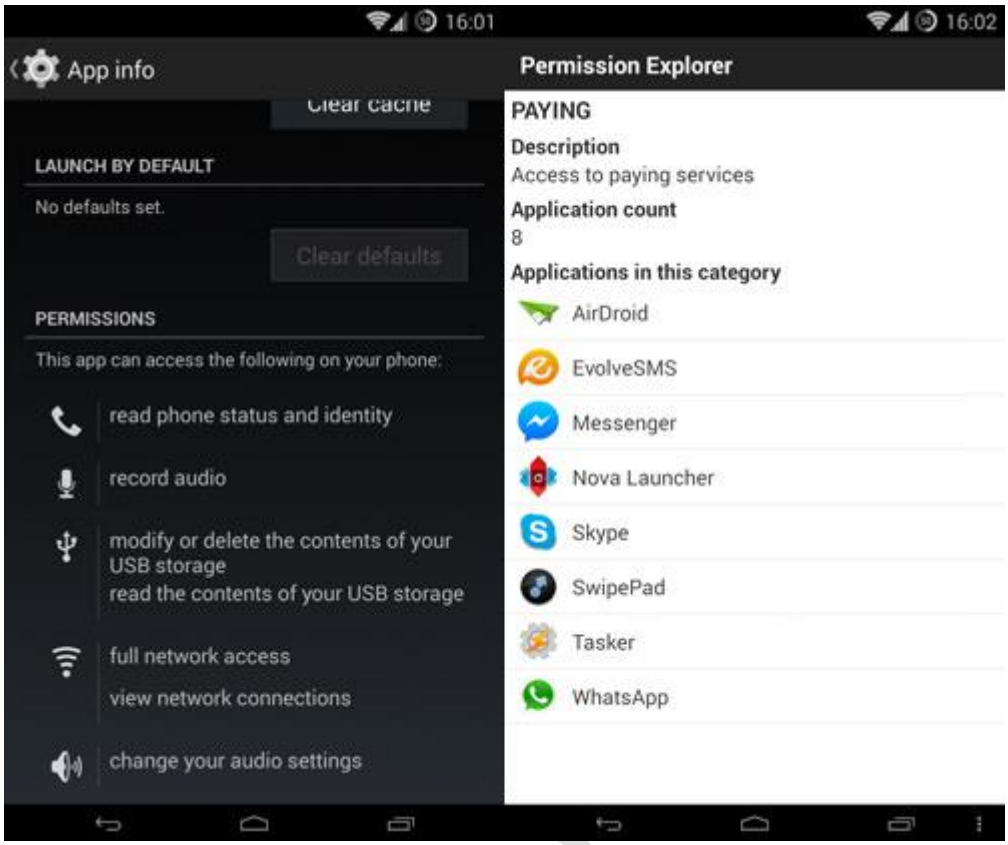
اگر شما به برنامه کاربردی اجازه دسترسی به حساب‌های کاربری خود را داده‌اید بهتر است مجوزهای حساب‌های کاربری خود را مدیریت کنید که این کار با رفتن به تنظیمات حساب کاربری و مشخص کردن مجوزها برای برنامه کاربردی موردنظر قابل‌حل خواهد بود.



شما همچنین می‌توانید با رفتن به Settings>Apps، مجوزهای اصلی برنامه‌های کاربردی را بررسی کنید. کافی است برنامه کاربردی موردنظر را انتخاب کنید و مجوزهای آن را مشاهده نمایید.

برنامه‌های کاربردی مدیریت مجوزها

شما همچنین می‌توانید از برنامه‌های کاربردی، همچون Permission Explorer برای مدیریت مجوزها استفاده کنید. این نوع از برنامه‌ها به شما این امکان را می‌دهند تا با اعمال یکسری فیلترها بر اساس **دسته‌بندی**، **برنامه کاربردی** و **مجوزها** شما را در مدیریت بهتر مجوزهای تفویض شده به برنامه کاربردی با جزئیات بیشتر آگاه سازد. از دیگر برنامه‌های مشابه می‌توان به Permissions Observatory و App Permissions اشاره نمود.



اندکی زمان را برای بررسی مجوزهای درخواستی برنامه کاربردی نصب‌شده بر روی دستگاه اندرویدی خود صرف نمایید، این کار باعث می‌شود تا برنامه‌هایی را که از مجوزهای مشکل‌ساز استفاده می‌کنند، شناسایی کرده و در مورد حذف و یا صحت کارکرد آن‌ها اقدامات لازم را انجام دهید.

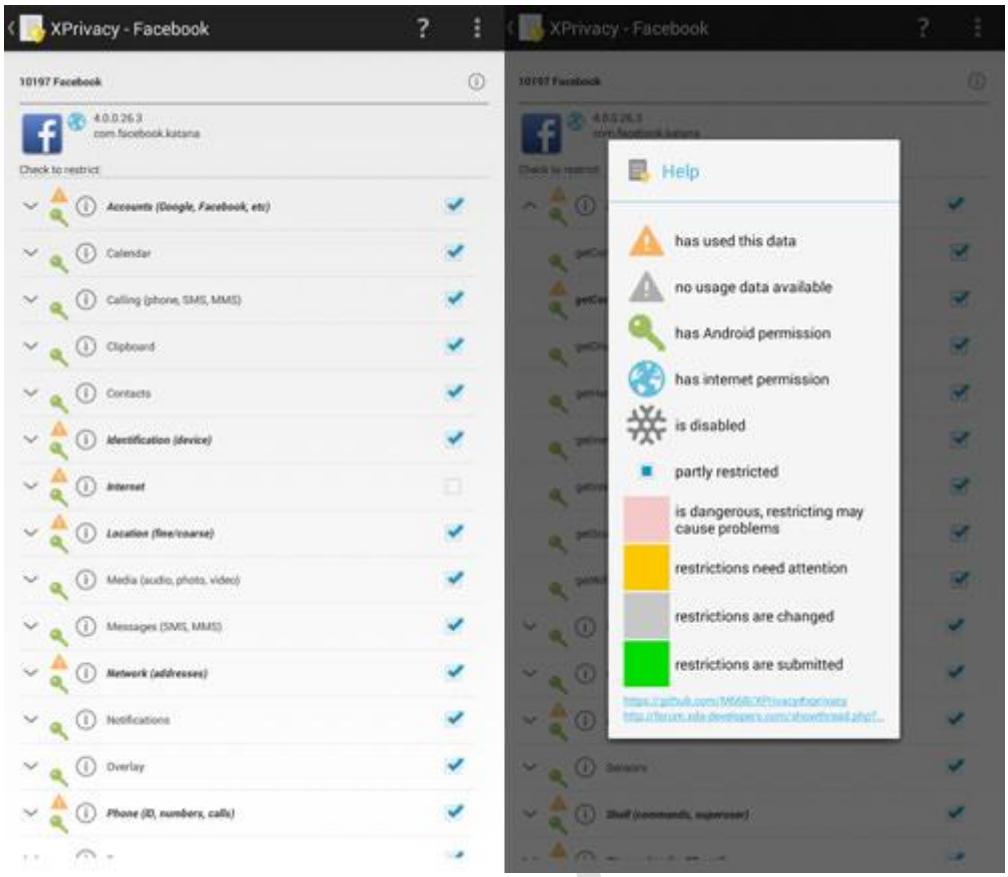
لغو مجوزهای برنامه کاربردی

هنگامی‌که شما برنامه کاربردی متخلف را شناسایی کردید اکنون زمان اتخاذ تصمیم مناسب است. به‌صورت پیش‌فرض روشی برای مدیریت مجوزهای برنامه کاربردی در نسخه‌های اندروید لحاظ نشده است و از نسخه ۴.۴.۲ اندروید، گوگل ویژگی AppOps را در سیستم‌عامل خود قرار داده است.

اگر شما همچنان از نسخه غیر روت شده ۴.۴.۲ و یا نسخه ۴.۳ اندروید استفاده می‌کنید شما توانایی حذف کامل برنامه‌های کاربردی که مجوزهای غیرمتعارف را دریافت کرده‌اند را خواهید داشت. البته اگر سیستم شما روت شده هم باشد باید گفت که گزینه‌های بیشتری برای شما وجود خواهد داشت تا با این دست مشکلات برخورد کنید.

برنامه‌های کاربردی مدیریت مجوزها (دستگاه‌های روت شده)

شما می‌توانید برنامه Xposed Framework یا برنامه XPrivacy را روی دستگاه خود نصب کنید. XPrivacy یکی از بهترین برنامه‌های کاربردی مدیریت مجوزهای برنامه کاربردی است که به‌راحتی قابل‌دسترسی بوده و به شما این اجازه را می‌دهد تا تمام مجوزهایی را که یک برنامه کاربردی ممکن است نیاز داشته باشد را لغو و یا ببندد. شما می‌توانید با استفاده از XPrivacy Installer هر دو برنامه Xposed Framework و XPrivacy به‌راحتی نصب کنید.



نتیجه‌گیری

درمجموع باوجود تعبیه شدن تنظیمات حریم خصوصی و امنیتی پیش‌فرض در دستگاه‌های مبتنی بر سیستم‌عامل اندروید، اندکی ضعف در این نوع تنظیمات دیده می‌شود. توسعه‌دهندگان برای افزایش قابلیت‌های کلیدی برنامه‌های کاربردی خود نیاز به دریافت تائید مجوز برای دسترسی به اطلاعات کاربر را دارند و متأسفانه به‌طور کامل نمی‌توان به توسعه‌دهندگان اطمینان داشت. راهکاری که می‌تواند کارساز باشد این است که کاربر مجوزهای موردنیاز برنامه‌های خود را به هنگام نصب بررسی کرده و به آن‌ها توجه ویژه‌ای داشته باشد به‌خصوص آن دسته از کاربرانی که برنامه‌های کاربردی خود را از فروشگاه‌های غیر معتبر دریافت می‌کنند.