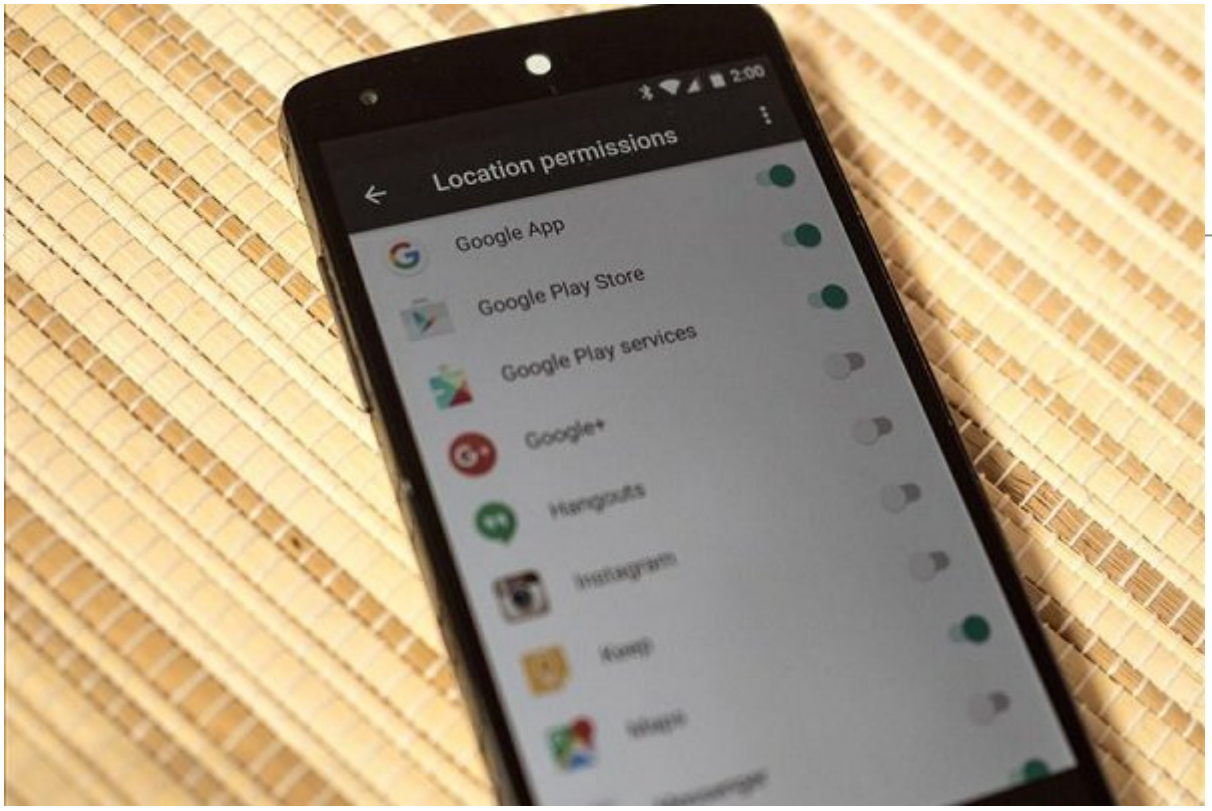
سطح دسترسی و مجوز چیست چه خطراتی دارد؟

مجوزهایی که به برنامه‌های اندرویدی می‌دهید، به امنیت گوشی شما آسیب می‌زند؟

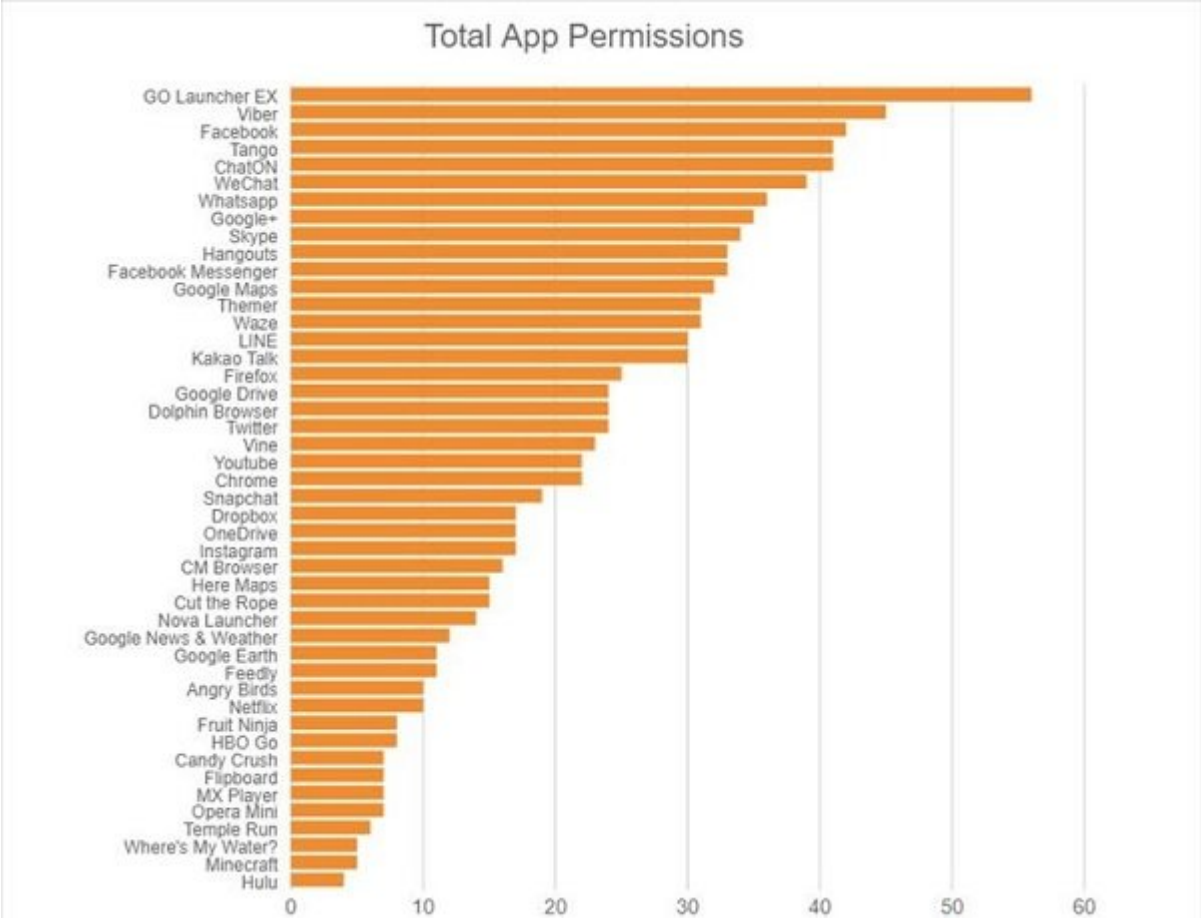


ما در این مقاله سعی خواهیم کرد شما را با مرسوم‌ترین و رایج‌ترین سطوح دسترسی که برنامه‌های کاربردی اندرویدی درخواست می‌کنند و تاثیر آن‌ها بر امنیت گوشی شما، آشنا کنیم.

تاکنون چندمرتبه پیش از آن‌که یک برنامه کاربردی را روی گوشی اندرویدی نصب کنید، موافقت‌نامه یا سطح دسترسی‌هایی را که یک برنامه درخواست کرده است، به‌دقت مطالعه کرده‌اید؟ اگر نسبت به این مسئله کم‌توجه هستید، باید بدانید که شما تنها کاربری نیستید که در این زمینه سهل‌انگار است. آمارها نشان می‌دهند، برای نیمی از کاربران مهم نیست که در زمان نصب چه مجوزها و سطح دسترسی‌هایی را به یک برنامه تخصیص می‌دهند. به‌عنوان مثال، ممکن است یک برنامه سرگرمی را نصب‌کرده باشید اما برنامه در زمان نصب از شما درخواست می‌کند تا به پیامک‌های روی گوشی شما دسترسی داشته باشد. اما دسترسی‌ها در اندروید چه معنایی می‌دهند و هر یک از این دسترسی‌ها ممکن است چه پیامدهایی برای ما به همراه داشته باشند؟

دسترسی‌هایی که بی‌مورد تخصیص داده می‌شوند

همان‌گونه که در مقدمه به آن اشاره داشتیم، کاربران اغلب به نیاز فعلی خود توجه می‌کنند و کمتر کاربری را پیدا می‌کنید که علاقه‌ای داشته باشد تا به تحقیق در ارتباط با مجوزها و سطوح دسترسی بپردازد که یک برنامه درخواست می‌کند. به عبارت ساده‌تر، کاربران همواره فرض را بر اصل اعتماد کردن به سازندگان برنامه‌ها قرار می‌دهند و همین موضوع باعث شده تا مشکلات مختلفی از نقض **حریم خصوصی** گرفته تا نصب بدافزارها روی گوشی‌های اندرویدی گریبان‌گیر بسیاری از کاربران شود. (شکل 1)



:1□□□
□□□□□□□
□□□
□□□□□□□
□□
□□□□□□□□
□□ □□□□
□□□□□□□□
□□□□
□□□□□
□□□□
□□□
□□□□
.□□□□□

سطح دسترسی و مجوز چیست؟

سطح دسترسی که در [سیستم‌عامل اندروید] با واژه **Permission** شناخته می‌شود، مکانیزمی است که به برنامه‌های کاربردی اجازه می‌دهد به منابعی همچون دوربین، کارت حافظه، پردازنده مرکزی و گرافیکی و.... دسترسی پیداکرده و از این منابع استفاده کنند. به‌عنوان مثال، اگر برنامه‌ای را روی گوشی اندرویدی خود نصب کنید تا برای هر مخاطب آهنگ خاصی را به صدا در آورد، به‌طورمعمول این برنامه باید به کارت حافظه و فهرست مخاطبان ذخیره‌شده روی دستگاه شما دسترسی داشته باشد. اگر این مجوزها به برنامه مذکور تخصیص داده نشود، شما قادر نخواهید بود از این برنامه استفاده کنید.

اما به‌راستی همه برنامه‌ها نیاز دارند تا سطح کاملی از دسترسی‌ها را به دست آورند؟ همه برنامه‌ها باید به بخش‌های مختلف یک گوشی دسترسی داشته باشند؟ قطعا این‌گونه نیست. اگر به فهرست برنامه‌های نصب‌شده روی گوشی اندرویدی خود مراجعه کرده و مجوزهایی را که هر یک از برنامه‌ها به دست آورده‌اند، بررسی کنید ممکن است در برخی موارد با موارد عجیب‌وغریب روبه‌رو شوید. به‌عنوان مثال، اگر به فهرست دسترسی و مجوزهای دریافت شده از سوی بازی‌های پرطرفداری همچون Cut the Rope مراجعه کنید، مشاهده می‌کنید که این برنامه مجوز دسترسی به موقعیت جغرافیایی یک کاربر را درخواست می‌کند، حال آن‌که مطابق با سیاست‌نامه منتشرشده از سوی شرکت سازنده بازی، این برنامه هیچ‌گاه اطلاعات مربوط به موقعیت جغرافیایی کاربران را جمع‌آوری نخواهد کرد.

کاملا روشن است که این اطلاعات به‌منظور ارائه تبلیغاتی هدفمند و متناسب با محل زندگی کاربران جمع‌آوری می‌شود. همچنین این اطلاعات به‌منظور به دست آوردن آماری از میزان استقبال کاربران از یک برنامه در کشورهای مختلف جمع‌آوری می‌شود. اما برای هر مجوزی که یک برنامه درخواست می‌کند به شکل روشنی نمی‌توان یک دلیل منطقی ارائه کرد. به‌عنوان مثال، برنامه‌ای شبیه Brightest Flashlight که تنها به‌منظور روشن کردن فلش گوشی‌های اندرویدی و تبدیل آن به یک چراغ‌قوه مورداستفاده قرار می‌گیرد، در پس‌زمینه اطلاعات مربوط به موقعیت جغرافیایی و همچنین دستگاهی را که مصرف‌کنندگان از آن استفاده می‌کنند، جمع‌آوری کرده و در ادامه این اطلاعات را به شرکت‌های فعال در زمینه انتشار تبلیغات می‌فروشد. اما این برنامه تنها نیست و دست‌کم هزاران برنامه این‌چنینی را می‌توان پیدا کرد.

مطلب پیشنهادی

انتقال تصاویر از گالری گوشی اندرویدی به پوشه ایمن
با این راهکار تصاویر خصوصی خود را روی گوشی اندرویدی پنهان کنید

با رایج‌ترین دسترسی‌های اندرویدی آشنا شوید

دسترسی‌های **اندروید** درجات مختلفی دارند و برخی از آن‌ها اگر به‌دقت بررسی نشوند، ممکن است کاربران را با مشکل جدی روبه‌رو کنند. در ادامه با برخی از رایج‌ترین دسترسی‌های **اندروید** آشنا خواهید شد.

دسترسی‌های که هزینه‌بر بوده و به شکل مستقیم تماس‌های تلفنی برقرار می‌کنند

این مجوز به معنای آن است که یک برنامه می‌تواند به‌طور خودکار یک تماس صوتی را برقرار کند. هر برنامه‌ای می‌تواند صفحه شماره‌گیری را اجرا کرده و حتی شماره‌های موردنظر خود را در آن وارد کند، اما تنها زمانی می‌تواند دکمه Dial را فشار دهد که شما به‌صراحت مجوز مربوطه را به آن واگذار کرده باشید. برنامه‌هایی همچون Google Voice یا Go Dialer به چنین سطحی از دسترسی نیاز دارند، اما اگر یک برنامه از شما درخواست چنین مجوزی را می‌کند، اما نباید چنین درخواستی را مطرح کند، پیش از دانلود آن از گوگل پلی تحقیقی انجام دهید تا از اصالت برنامه اطمینان حاصل کنید.

دسترسی‌هایی که هزینه‌بر بوده و برای ارسال پیام‌های کوتاه متنی و تصویری درخواست می‌شوند

این سطح از دسترسی ممکن است به‌منظور ارسال و دریافت پیام درخواست شود. یکسری از برنامه‌های کاربردی به‌گونه‌ای طراحی‌شده‌اند که مخاطب خود را ناخواسته به فهرست پیامکی وارد کرده و به این شکل هزینه‌های سنگینی روی دست مصرف‌کننده باقی می‌گذارند. دقت کنید برنامه‌هایی که به شما اجازه می‌دهند از درون برنامه کاربردی پیام کوتاه یا پیام چندرسانه‌ای ارسال کنید به این سطح از دسترسی نیاز دارند، همچنین برنامه‌هایی که قابلیت به اشتراک‌گذاری محتوای چندرسانه‌ای را دارند، به چنین مجوزی نیاز خواهند داشت، اما به سایر برنامه‌ها هیچ‌گاه نباید چنین سطح از دسترسی را تخصیص دهید. شما در زمان نصب یک برنامه و با توجه به عملیاتی که یک برنامه انجام می‌دهد به‌راحتی می‌توانید این موضوع را متوجه شوید.

دسترسی‌های مرتبط با اطلاعات شخصی- خواندن/نوشتن به فهرست مخاطبان

یک برنامه کلاینت ایمیلی یا یک برنامه پیام‌رسان از این مجوز به‌منظور خواندن فهرست مخاطبان استفاده می‌کند. این سطح از مجوزها به سه گروه مجوزهای دسترسی به‌منظور خواندن و نوشتن به فهرست مخاطبان، خواندن و نوشتن به رخدادهای تقویم و تغییر یا ویرایش اطلاعات حافظه تقسیم می‌شوند. به‌عنوان مثال، برنامه‌های پیام‌رسان و ایمیل نیاز دارند به اطلاعات فهرست مخاطبان دسترسی داشته باشند. برنامه‌هایی همچون پیام‌رسان‌ها نیز برای پیدا کردن دوستان شما به مجوز دسترسی به فهرست مخاطبان نیاز دارند. در حوزه سرگرمی بازی‌هایی که در آن‌ها فهرست رتبه‌بندی شده بازیکنان قرار دارد، به این سطح از دسترسی نیاز دارند. در ارتباط با این مدل برنامه‌ها مجوز نوشتن به فهرست مخاطبان نیز وجود دارد. به‌عنوان مثال، اگر برنامه‌ای روی گوشی نصب کرده‌اید و در نظر دارید در این برنامه اسم فردی را به فهرست مخاطبان خود اضافه کنید، طبیعی است که این برنامه به دسترسی نوشتن به فهرست مخاطبان نیاز خواهد داشت.

دسترسی به اطلاعات شخصی- خواندن/نوشتن رخدادهایی به تقویم

درخواست این سطح از مجوزها سرراست بوده و به‌راحتی می‌توانید ماهیت آن را درک کنید. این سطح از مجوزها تنها یک کار انجام می‌دهد، به‌منظور خواندن یا نوشتن رخدادهایی به تقویم مورداستفاده قرار می‌گیرد. برنامه‌های مربوط به یادآوری رخدادها نیاز دارند تغییراتی در تقویم به وجود آورند. همچنین برنامه‌هایی که قرار است کارهایی را در زمان‌های مشخصی انجام دهند به چنین سطح از دسترسی نیاز خواهند داشت. اگر برنامه‌ای را نصب کردید که چنین کارهایی را انجام نمی‌دهد، اما در مقابل درخواست چنین سطح از دسترسی را می‌کند، بهتر است راهنمای برنامه را مطالعه کرده یا در صورت امکان از تولیدکننده برنامه در این خصوص سوال کنید.

مطلب پیشنهادی

مقایسه اجازه دسترسی ده پیام‌رسان مهم داخلی و خارجی
چرا پیام‌رسان‌ها برای نصب به این همه اجازه دسترسی نیاز دارند؟ مقایسه دسترسی‌های پیام‌رسان‌های داخلی و خارجی

دسترسی به اطلاعات شخصی در ارتباط با کارت حافظه

دسترسی مربوط به خواندن و نوشتن اطلاعات روی کارت حافظه در اغلب موارد با عبارت‌هایی شبیه Delete/Modify SD card contents نشان داده می‌شوند. برخی از کاربران به‌اشتباه این‌گونه تصور می‌کنند زمانی که عبارت کارت حافظه نشان داده می‌شود منظور فقط اعمال تغییرات روی کارت حافظه است، حال آن‌که این پیام حافظه اصلی گوشی را نیز شامل می‌شود. بدافزارها از رایج‌ترین نرم‌افزارهایی هستند که برای دسترسی به اطلاعات کاربران، حذف اطلاعات یا تغییر اطلاعات چنین سطح از دسترسی را طلب می‌کنند. درحالی‌که گوگل در تلاش است تا این سطح از دسترسی را با مخاطرات کمتری همراه کند و تقریبا با ارائه هر نسخه از **اندروید** نحوه دسترسی برنامه‌ها به اطلاعات را ویرایش می‌کند، با این حال هنوز هم کاربرانی وجود دارند که از نگارش‌های قدیمی **اندروید** استفاده می‌کنند و تخصیص چنین سطح از دسترسی از سوی کاربران مخاطره‌آمیز است. درحالی‌که در نسخه‌های قدیمی همه برنامه‌ها به شکل خودکار چنین سطح از دسترسی را دارند، اما تعداد این برنامه‌ها زیاد نیست. بااین‌حال، اگر روی گوشی اندرویدی برنامه‌ای خارج از پلی‌استور را نصب کرده‌اید ممکن است ناخواسته چنین سطح از دسترسی را واگذار کرده باشید. اندروید از نسخه هفت به بعد سطح دسترسی برنامه‌ها به حافظه را کاملا محدود کرده است.

مجوز دسترسی به وضعیت و اطلاعات فنی گوشی (اطلاعات شماره سریال کارخانه‌ای گوشی)

بسیاری از کاربران با تخصیص چنین مجوزی آشنایی زیادی ندارند و همین مسئله باعث شده برخی از برنامه‌ها از کم‌اطلاعی کاربران در این زمینه سوءاستفاده کنند. باید بدانید که این مجوز دو گروه متفاوت از اطلاعاتی را که با یکدیگر متفاوت هستند، شامل می‌شود. گروه اول اطلاعاتی است که برای تعیین و تشخیص وضعیت گوشی مورداستفاده قرار می‌گیرد. به‌عنوان مثال، یک بازی را فرض کنید که در نظر دارد جای خود را به صفحه تماس بدهد. برای تغییر این برنامه باید به وضعیت گوشی دسترسی داشته باشد. گروه دوم، اطلاعاتی است که دسترسی به آن‌ها از طریق این مجوز که در ارتباط با شناسه منحصربه‌فرد یک گوشی است، انجام می‌شود. هر گوشی هوشمندی یک شناسه دارد که یک گوشی را از دیگری متمایز می‌کند. این شناسه بدون آن‌که اطلاعات شخصی کاربری را به اشتراک قرار دهد از سوی یک برنامه می‌تواند مورداستفاده قرار گیرد.

زمانی که مشاهده می‌کنید چه تعداد از مردم از یک نسخه خاص از اندروید استفاده می‌کنند این آمار با استناد به این شناسه به دست می‌آید. تعداد کاربرانی که به فروشگاه گوگل پلی وارد می‌شوند، با استناد به این شناسه شمارش می‌شوند. از این شناسه برای تشخیص اطلاعاتی که روی سرویس‌های ابری ذخیره‌شده است، استفاده می‌شود. اما از این سطح دسترسی برای خواندن اطلاعات دیگری که همانا شناسه IMEI است، استفاده می‌شود. این شناسه کاربر واقعی را با گوشی **اندرویدی** که از آن استفاده می‌کند، مرتبط می‌کند. به‌عنوان مثال، اگر گوشی شما به سرقت رفت، اپراتورها با این شناسه قادر هستند گوشی را غیرفعال کرده یا برای پیدا کردن آن اقدام کنند. عملکرد شناسه IMEI چیزی شبیه شماره شاسی خودرو است. درحالی‌که دسترسی به چنین شناسه‌ای کار چندان راحتی نیست، اما غیرممکن نیست. با توجه به این‌که به‌درستی مشخص نیست یک برنامه ممکن است به کدام‌یک از این اطلاعات دست پیداکرده و برای چه منظوری از این اطلاعات استفاده کند، در نتیجه پیشنهاد می‌کنیم در زمان تخصیص این دسترسی مجوز احتیاط کنید.

دسترسی به ارتباط شبکه‌ای

بدون هیچ‌گونه توضیح اضافی مشخص است که این دسترسی به چه منظور درخواست می‌شود. هر برنامه‌ای که در نظر داشته باشد به اینترنت متصل شود چنین مجوزی را درخواست خواهد کرد. برنامه‌هایی که رایگان بوده اما در زمان نصب اعلام می‌دارند تبلیغاتی را به کاربر نشان خواهند داد چنین مجوزی را درخواست خواهند کرد. این سطح از دسترسی در حالت عادی اطلاعات شخصی شما را در معرض خطر قرار نمی‌دهد، اما ممکن است بدون اطلاع شما حجم بالایی از اینترنت شما را مصرف کند. به‌ویژه برنامه‌هایی که به‌طور مرتب به‌روز شده یا بانک اطلاعاتی

خود را دائم به‌روز می‌کنند. البته توجه داشته باشید که در برخی موارد یکسری برنامه‌های مشکوک از این مجوز ممکن است برای نصب نرم‌افزارهای ناخواسته یا حتی دانلود بدافزارها روی گوشی استفاده کنند.

مجوز دسترسی به موقعیت جغرافیایی

برخی از برنامه‌ها برای تعیین موقعیت جغرافیایی کاربر از همان اطلاعات مربوط به وای‌فای استفاده می‌کنند، اما برخی از برنامه‌ها به موقعیت جغرافیایی دقیق یک کاربر نیاز دارند. برنامه‌هایی شبیه تناسب‌اندام برای آن‌که بتوانند فاصله نقطه شروع و خاتمه دویدن یک فرد را محاسبه کنند، به چنین مجوزی نیاز دارند. برنامه‌هایی نظیر نقشه‌ها به چنین مجوزی نیاز دارند. برنامه‌هایی که ویژه افراد کم‌توان جسمی طراحی‌شده دسترسی به چنین مجوزی را درخواست می‌کنند. برنامه‌هایی که در آن‌ها تبلیغات نشان داده می‌شود نیز به چنین مجوزی نیاز دارند که البته این مورد با توجه به انتخاب شخصی شما می‌تواند واگذارشده یا رد شود.

مطلب پیشنهادی

ادعای کذب سازندگان اسمارت‌فون‌های اندروید در خصوص به‌روزرسانی‌های امنیتی
خیلی از به‌روزرسانی‌های اندروید فاقد وصله‌های امنیتی گزارش شده هستند

گوگل را فراموش نکنید

اگر جزو آن گروه از کاربرانی هستید که برنامه‌های خود را تنها از فروشگاه پلی استور دریافت می‌کنید باید بدانید که **گوگل** در این زمینه کاملا مراقب است. **گوگل** سعی می‌کند به کاربران خود این اطمینان خاطر را بدهد که برنامه‌های دانلود شده از این فروشگاه **حریم خصوصی** کاربران را در معرض خطر قرار نمی‌دهد. البته راهکاری برای تشخیص این موضوع که یک برنامه ایمن است یا خیر وجود دارد. شما از طریق رتبه تخصیص داده‌شده از سوی کاربران به یک برنامه و تعداد دانلودهای یک برنامه در فروشگاه گوگل‌پلی می‌توانید از ایمن بودن آن اطمینان حاصل کنید. همچنین اگر گزینه منابع ناشناس (Unknown Sources) در بخش **امنیت** روی تنظیمات گوشی خود را فعال نکرده باشید خطر چندانی شما را در ارتباط با مجوزهای سطح دسترسی تهدید نمی‌کند. خوشبختانه از نسخه ششم به بعد **سیستم‌عامل اندروید** فرآیند دریافت مجوزهای دسترسی از سوی یک برنامه به‌یک‌باره انجام‌نشده و هر زمان برنامه‌ای تصمیم بگیرد از قابلیت جدیدی استفاده کند، اندروید به شما اعلام می‌دارد که برنامه به مجوز دیگری نیاز دارد.

گوگل به دنبال آن است تا از شرکت‌ها به‌روزرسانی‌های امنیتی منظم را درخواست کند

به نظر می‌رسد، **گوگل** در زمینه **امنیت** کاربران کاملا مصمم است. دیو کیلیر مارچ، درست از اوایل سال جاری که به سمت مدیر بخش امنیت اندروید منصوب شد، در کنفرانس توسعه‌دهندگان امسال **گوگل** اعلام کرد: «ما به دنبال آن هستیم تا مبحث **امنیت** در اندروید را دگرگون کرده و آن‌را بهتر کنیم. ما از شرکت‌های تولیدکننده دستگاه‌های اندرویدی درخواست خواهیم کرد به‌روزرسانی‌های **امنیتی** را به شکل منظم ارائه کنند و در نظر داریم بند جدیدی را به توافقنامه‌ای که با شرکت‌های تولیدکننده گوشی منعقد کرده‌ایم اضافه کنیم که به‌موجب آن شرکت‌ها وصله‌های امنیتی را به شکل دقیق برای محصولات خود ارائه کنند. این سیاست باعث خواهد شد گوشی‌های بیشتری بتوانند وصله‌های امنیتی را دریافت کنند که این موضوع **امنیت** دستگاه‌ها را بهبود خواهد بخشید. به‌طوری‌که دستگاه‌ها در بازه‌های زمانی 90 روزه وصله‌های امنیتی را دریافت کنند.» بدون شک این اقدام **گوگل** ضمن آن‌که به بهبود **امنیت** گوشی‌ها منجر خواهد شد، به برنامه‌ها نیز اجازه نخواهد داد به‌واسطه نبود وصله‌های امنیتی از مجوزهایی که به دست آورده‌اند، سوءاستفاده کنند.

منبع:
androidpolice
androidcentral
blog.zedge
androidauthority
imei-number
تاریخ انتشار:
28 اردیبهشت 1398

نشانی منبع:
https://www.shabakeh-mag.com/security/13941/%D9%85%D8%AC%D9%88%D8%B2%D9%87%D8%A7%DB%8C%DB%8C-%DA%A9%D9%87-%D8%A8%D9%87-%D8%A8%D8%B1%D9%86%D8%A7%D9%85%D9%87%E2%80%8C%D9%87%D8%A7%DB%8C-%D8%A7%D9%86%D8%AF%D8%B1%D9%88%DB%8C%D8%AF%DB%8C-%D9%85%DB%8C%E2%80%8C%D8%AF%D9%87%DB%8C%D8%AF%D8%8C-%D8%A8%D9%87-%D8%A7%D9%85%D9%86%DB%8C%D8%AA-%DA%AF%D9%88%D8%B4%DB%8C-%D8%B4%D9%85%D8%A7-%D8%A2%D8%B3%DB%8C%D8%A8-%D9%85%DB%8C%E2%80%8C%D8%B2%D9%86%D8%AF%D8%9F