

قابلیت جدید اندروید ۱۴ برای مقابله با هکرها

اندروید ۱۴ با انبوهی از ویژگی‌های جدید همراه خواهد بود اما یکی از مهم‌ترین آن‌ها، مربوط به جلوگیری از حملات فیشینگ و افشای اطلاعات کاربران خواهد بود.

به گزارش سایت خبری پرسون، نسخه جدید اندروید مجهز به قابلیت‌های جدید و متنوعی شده و کاربران زیادی با انتشار اولین بتای عمومی آن، در حال تست و بررسی ویژگی‌های جدید سیستم عامل هستند. در این به روز رسانی دسترسی و تعامل با گوشی بسیار راحت‌تر شده و برای نمونه متن‌ها با رنگ کنتراست بالایی نمایش داده می‌شوند که در واقع بخشی از رابط کاربری جدید اندروید یعنی Material You و Material You ۲ به حساب می‌آید.

در این میان هکرهایی مانند تیم Nexus یا Cerberus که به تولید بدافزار اندرویدی مشغول هستند، از این ویژگی جدید سیستم عامل سواستفاده کرده‌اند. خوشبختانه گوگل در اندروید ۱۴ ابزاری در آستین دارد تا دست هکرها از اطلاعات شخصی کاربران کوتاه بماند.

سرویس‌های دسترسی که آن‌ها را با نام Accessibility می‌شناسیم در API اندروید باقی مانده‌اند تا کاربرانی که با ناتوانی دست و پنجه نرم می‌کنند، علی‌رغم توانایی ارتباط کم با گوشی همچنان بتوانند از آن استفاده کنند. این سرویس شامل مواردی مانند Voice Access، TalkBack و Select to Speak می‌شود اما برنامه‌های دیگر می‌توانند ویژگی‌های مختص به خودشان را نیز ارائه کنند.

برای ایجاد راحتی بیشتر برای کاربران، سرویس‌های Accessibility از برنامه‌های دیگر اجازه می‌گیرند تا بتوانند به محتوای آن اپ دسترسی داشته باشند و آن را بخوانند. اما این دسترسی‌ها به دلیل ماهیتشان فراتر از دسترسی‌های عادی هستند و ویژگی Screen Reader ممکن است به بدافزار اندرویدی اجازه بدهد تا کدهای دو عاملی ۲FA را بخواند و بدزدد. این متد می‌تواند حتی برنامه Google Authenticator را نیز تحت تاثیر قرار بدهد و رمز کاربر را افشا کند.

یکی از متخصصان اندروید، Mishaal Rahman می‌گوید اندروید ۱۴ مکانیسم جدیدی را معرفی می‌کند که اجازه دسترسی برنامه‌های مخرب و آسیب‌زا به اطلاعات امنیتی مهم دستگاه مانند کدهای احراز هویت دو عاملی را صادر نمی‌کند. همچنین اندروید از فعالسازی آسان دسترسی‌های Accessibility حتی توسط برنامه‌هایی که از فروشگاه‌های نرم افزاری ثالث دانلود شده‌اند هم جلوگیری خواهد کرد. بدین ترتیب اگر برنامه‌ای نصب کنید که بخواهد از ویژگی‌های Accessibility استفاده کند، بایستی شخصا اجازه دسترسی اپلیکیشن به محتوای روی صفحه را بدهید تا از احتمال سواستفاده هکرها کاسته شود.

رحمان ادامه می‌دهد این API جدید با نسخه‌ای که در پیش‌نمایش دوم توسعه‌دهندگان منتشر شده بود تفاوت‌هایی دارد. گرچه این ویژگی تقریباً به همان روال قبل کار می‌کند اما در بتای جدید اندروید ۱۴ هوشمندتر شده و می‌تواند تصمیم بگیرد چه دیتایی جزو اطلاعات شخصی و امنیتی است. بدین ترتیب اگر برنامه‌ای بخواهد بدون اجازه به آن دسترسی پیدا کند، سیستم به طور خودکار دسترسی آن را بلاک خواهد کرد. همچنین تنظیمات دیگری هم وجود دارند تا توسعه‌دهندگان بتوانند دسترسی به سرویس‌های Accessibility را از بین ببرند.

بدین ترتیب سرویس‌هایی مانند TalkBack به کار خودشان ادامه می‌دهند اما دسترسی بدافزارها به اطلاعاتی مانند کدهای ۲FA قطع خواهد شد. این تنظیمات به طور خودکار اعمال می‌شوند و حتی اگر یک توسعه‌دهنده به سراغ رعایت چنین کدها و ویژگی‌های امنیتی نرود، خود سیستم عامل مانع از افشای اطلاعات کاربر خواهد شد.

گرچه تلاش گوگل برای پیشگیری از اتفاقات ناگوار در اندروید ۱۴ تحسین‌برانگیز است اما باید بدانید اگر خودتان نسبت به امنیت موبایل‌تان حساسیت به خرج ندهید، هیچ ویژگی امنیتی نمی‌تواند شما را نجات بدهد. بیشتر ویژگی‌های امنیتی تنها بازدارنده هستند و بالاخره هکرها به سراغ راه‌های دیگری برای نفوذ به اطلاعات دیوایس شما خواهند رفت. بنابراین هوشیار باشید و اپلیکیشن‌هایتان را فقط از فروشگاه‌های نرم افزاری معتبر مانند گوگل پلی استور دانلود کنید.