# راهکارهای آزمایش شده برای محافظت از گوشی های اندرویدی در برابر تهدیدات امنیتی (بخش اول)


در حالی که عده‌ای از کارشناسان حوزه امنیت بر این بار هستند که امنیت گوشی‌های اندرویدی در سطح بسیار بالایی قرار دارد، با این وجود عده‌ای از کاربران محصولات اپل می‌گویند که آی‌فون‌ها و به ویژه سیستم‌عامل iOS در این زمینه بدون رقیب هستند. اما اگر به اخبار حوزه امنیت نگاهی داشته باشید مشاهده می‌کنید که این‌گونه نیست. به‌طور مثال زمانی که اپل از سیستم‌عامل iOS نگارش 11 رونمایی کرد، درست یک روز پس از عرضه رسمی متخصصان امنیتی ژاپنی توانستند 2 آسیب‌پذیری مهم را در سیستم‌عامل تازه‌وارد اپل شناسایی کنند و با استفاده از این آسیب‌پذیری‌ها به آی‌فون‌های اپل نفوذ کنند. اما این حرف به معنای آن نیست که سیستم‌عامل اندروید عاری از هرگونه آسیب‌پذیری است و هکرها قادر نیستند به آن نفوذ کنند. سیستم‌عامل اندروید نیز به‌طور پیوسته آماج حملاتی می‌شود که از سوی هکرها ترتیب داده شده است. به ویژه نگارش‌های قدیمی‌تر این سیستم‌عامل که به آسیب‌پذیری‌های بیشتری گرفتار هستند و در بعضی موارد هیچ‌گونه وصله امنیتی برای ترمیم این آسیب‌پذیری‌ها ارائه نشده است.

**قسمت دوم این مقاله را می‌توانید در اینجا ببینید.**

در حالی که گوگل به‌طور ماهانه وصله‌هایی را برای ترمیم آسیب‌پذیری‌های اندروید ارائه می‌کند، اما واقعیت این است که برخی از تولیدکنندگان گوشی‌های اندرویدی وصله‌ها را در اسرع وقت ارائه نکرده یا برخی از آن‌ها نسبت به عرضه به‌روزرسانی‌ها برای محصولاتی که تولید کرده‌اند بی تفاوت هستند. به ویژه محصولاتی که قدیمی بوده و به اعتقاد این شرکت‌ها دیگر ارزشی ندارد برای آن‌ها به‌روزرسانی ارائه شود. در چنین شرایطی و با توجه به انواع مختلف حملات هکری که شاهد آن‌ها هستیم این خود کاربران گوشی‌های هوشمند هستند که باید از طریق به‌کارگیری تهمیدات لازم از گوشی‌های خود در برابر حملات هکری محافظت به عمل آورند. سایت ZdNet یکی از معتبرترین سایت‌های خبری‌تحلیلی است که مقالات متعدد و متنوعی در حوزه‌های مختلف و به ویژه مبحث امنیت منتشر می‌کند. این سایت چندی پیش مقاله‌ای در ارتباط با ایمن‌سازی گوشی‌های اندرویدی منتشر کرد و در این مقاله به معرفی ده راهکاری پرداخت که در عین سادگی به خوبی قادر هستند از گوشی‌های ما محافظت به عمل آورند. ما در این مقاله ضمن بررسی این ده راهکار مفید، به شما نشان خواهیم داد که چگونه می‌توانید گذرواژه‌های قدرتمندی را ایجاد کرده و از این گذرواژه‌ها در برنامه‌های مختلف و به ویژه گوشی‌های اندرویدی خود استفاده کنید.

## 1.گوشی‌هایی را خریداری کنید که وصله‌های امنیتی اندروید را به‌طور مستمر دریافت می‌کنند

بدون شک یکی از بهترین مثال‌هایی که در این زمینه می‌توان به آن اشاره کرد گوگل پیکسل 2 است. این گوشی ویژگی‌های مثبت و منفی مختلفی دارد، اما یکی از مهم‌ترین ویژگی‌های شاخص گوشی‌های ساخت شرکت گوگل همچون پیکسل 2، نکسوس ایکس 5 و نکسوس پی 6 در ارتباط با دریافت مستمر به‌روزرسانی‌هایی است که این

گوشی‌ها دریافت می‌کنند. سایت Android Authority در مطلبی تحت عنوان کدامیک از تولیدکنندگان گوشی‌های هوشمند به‌روزرسانی‌ها را در اسرع وقت برای گوشی‌های خود عرضه می‌کنند فهرستی از تولیدکنندگان گوشی‌های هوشمند را منتشر کرد و در این گزارش به شکل دقیق نشان داده است که هر یک از تولیدکنندگان گوشی‌های هوشمند در چه بازه زمانی به‌روزرسانی نوقا را برای گوشی‌های خود عرضه کرده‌اند. در این گزارش آماده است که ال‌جی با تاخیری 78 روزه برای LG G5، موتورولا با تاخیری 88 روزه برای Moto Z، اچ‌تی‌سی با تاخیری 95 روزه برای HTC 10، سونی با تاخیری 99 روزه برای Xperiz XZ، شیائومی با تاخیری 126 روزه برای Mi 5، وان‌پلاس با تاخیری 131 روزه، برای OnePlus 3T سامسونگ با تاخیری 143 روزه  برای گلکسی س7 و اس7 اج به‌روزرسانی‌ها را برای محصولات خود عرضه کردند.

## 2. گوشی خود را قفل کنید

در حالی که قفل کردن گوشی یکی از بهترین راهکارهایی است که پیش روی کاربران وجود دارد، اما واقعیت این است که هنوز هم طیف گسترده‌ای از کاربران تمایلی به انجام این‌کار ندارند. گزارشی که چندی پیش منتشر شد نشان داد که هنوز هم آمار به سرقت رفتن داده‌های شخصی از طریق بدافزارهایی که به گوشی‌های هوشمند حمله می‌کنند در مقایسه با گوشی‌هایی که در خیابان‌ها به سرقت رفته و داده‌های آن‌ها در اختیار افراد سودجو قرار می‌گیرد قابل مقایسه نیست. اما پرسشی که مطرح می‌شود این است که چه راهکاری برای قفل کردن گوشی ایده‌آل است؟ بدون شک هنوز هم به‌کارگیری گذرواژه‌ها ایده‌آل‌ترین روشی است که پیش روی ما قرار دارد. در حالی که اکثر شرکت‌ها مکانیزم‌هایی همچون اثرانگشت، الگوی تشخیص صدا، اسکن عنبیه چشم و سایر مکانیزم‌های زیستی را پیشنهاد می‌دهند، اما واقعیت این است که مکانیزم‌هایی که به آن‌ها اشاره شد نیز در برابر حملات هکری آسیب‌پذیر بوده و مهم‌تر از آن اگر اثرانگشت شما به سرقت برود برای همیشه اثرانگشت شما در اختیار هکرها قرار خواهد گرفت. برای انتخاب یک گذرواژه قدرتمند راهکارهایی وجود که در انتهای مقاله به تعدادی از این راهکارها اشاره خواهیم کرد.

## 3. از مکانیزم احراز هویت دو مرحله‌ای استفاده کنید

پس از آن‌که گوشی خود را از طریق گذرواژه قفل کردید، در مرحله بعد بهتر است از مکانیزم احراز هویت دو مرحله‌ای برای قفل کردن حساب‌های کاربری و سرویس‌های گوگل استفاده کنید. بهترین راهکاری که در این زمینه پیش روی شما قرار دارد به‌کارگیری مکانیزم احراز هویت دو مرحله‌ای است که از سوی خود گوگل ارائه شده است. برای آن‌که ویژگی یاد شده در گوگل را فعال کنید، باید به تنظیمات حساب کاربری خود در گوگل رفته، در ادامه به بخش two-step verification  مراجعه کرده و از منوی ظاهر شده گزینه Using 2-step verification را انتخاب کنید. پس از انجام این‌کار از شما شماره تلفن همراه درخواست می‌شود. پس از وارد کردن شماره گوشی، کد مخصوص یکبار مصرفی از طریق پیام کوتاه برای گوشی شما ارسال می‌شود. در مرحله بعد باید پین‌کد دریافتی را در بخش موردنظر وارد کنید. در ادامه از شما سوال می‌شود که آیا در نظر دارید گوگل کامپیوتری که از آن استفاده می‌کنید را به مدت 30 روز به یاد آورد تا برای هر مرتبه ورود نیازی به ارسال کد نباشد. در ادامه می‌توانید گزینه بله را انتخاب کنید تا فرآیند کامل شود. برای اطلاعات بیشتر در این خصوص به آدرس https://myaccount.google.com/signinoptions/two-step-verification/enroll-... مراجعه کنید. راهکار دیگری که برای ایمن‌سازی در اختیار شما قرار دارد به‌کارگیری Google Prompt است. در این حالت، هر زمان به برنامه‌های مختلف گوگل وارد شوید، گزینه‌ای روی گوشی شما ظاهر می‌شود که با لمس گزینه بله اجازه دسترسی به آن برنامه امکان‌پذیر می‌شود.

## 4.  تنها از منابعی که قابل اطمینان هستند برنامه‌های خود را دانلود کنید

فروشگاه‌های مختلفی برای دانلود برنامه‌های اندرویدی وجود دارند که اغلب آن‌ها آلوده به بدافزارهای اندرویدی هستند. البته این به معنای آن نیست که فروشگاه پلی استور گوگل عاری از هرگونه بدافزاری است. در این فروشگاه نیز بدافزارهایی ممکن است پیدا شوند، اما این اتفاق تنها در شرایط خاصی روی می‌دهد و هنوز هم پلی استور ایمن‌ترین منبع برای دریافت برنامه‌ها است. گوگل برای آن‌که کاربران اکوسیستم اندروید در امان باشند همواره از راهکاهای جدید و به ویژه الگوریتم‌ها یادگیری ماشینی برای شناسایی قطعه کدها و برنامه‌هایی که به بدافزارها آلوده هستند استفاده می‌کند. به‌طور مثال، در فروشگاه گوگلی پلی بخشی به نام Google Play Protect وجود دارد که به شکل خودکار دستگاه‌های اندرویدی را به لحاظ آلوده بودن به بدافزارها مورد بررسی قرار می‌دهد. برای آن‌که اطمینان حاصل کنید که این ویژگی در دسترس شما قرار دارد در فروشگاه گوگل به مسیر Settings > Security

Play Protect > رفته و گزینه Play Protect را فعال کنید. برای آن‌که به حداکثر امنیت ممکن دست پیدا کنید پیشنهاد می‌کنیم گزینه‌های Full scanning و Scan device for security threats را هم فعال کنید.

## 5. از مکانیزم رمزگذاری دستگاه استفاده کنید

در شرایطی که قفل کردن گوشی مانع از آن می‌شود تا افراد غیرمجاز به گوشی شما دسترسی پیدا کنند، با این وجود هنوز هم راهکارهای دیگری وجود دارد که باعث می‌شوند امنیت دستگاه شما دوچندان شود. درست است که به‌کارگیری گذرواژه‌ها از گوشی شما محافظت به عمل می‌آورند اما اگر گوشی شما گم شده یا به سرقت برود، هکرها قادر هستند از طریق نرم‌افزارهای شکستن گذرواژه‌ها و از طریق به‌کارگیری تکنیک‌هایی همچون حملات جست‌وجوی فراگیر گذرواژه گوشی شما را شکسته و به آن وارد شوند. برای آن‌که به هکرها اجازه ندهید پس از شکستن قفل گوشی به داده‌های شخصی شما دست پیدا کنند باید از قابلیت رمزگذاری داده‌ها استفاده کنید. این راهکار ضریب ایمنی گوشی و داده‌هایی که روی آن قرار دارد را دوچندان می‌کند. به واسطه آن‌که هکرها تنها در صورتی می‌توانند به اطلاعات رمزگذاری شده دست پیدا کنند که کلید مربوط به رمزگشایی را در اختیار داشته باشند. برای فعال‌سازی این ویژگی باید به بخش تنظیمات گوشی خود رفته و در ادامه به بخش Security بروید. در این بخش گزینه‌ای به نام Encrypt Device قرار دارد که برای رمزگذاری داده‌ها می‌توانید از آن استفاده کنید. در کنار گزینه یاد شده برنامه‌های ویژه‌ای نیز برای این منظور وجود دارند که به شما اجازه می‌دهند داده‌هایی که روی گوشی یا کارت حافظه قرار دارید را رمزگذاری کنید.

**قسمت دوم این مقاله را می‌توانید در اینجا ببینید.**
**تاریخ انتشار:**

13 آذر 1398

---

**نشانی منبع:**
https://www.shabakeh-mag.com/tricks/mobile-tricks/16325/%D8%B1%D8%A7%D9%87%DA%A9%D8%A7%D8%B1%D9%87%D8%A7%DB%8C-%D8%A2%D8%B2%D9%85%D8%A7%DB%8C%D8%B4-%D8%B4%D8%AF%D9%87-%D8%A8%D8%B1%D8%A7%DB%8C-%D9%85%D8%AD%D8%A7%D9%81%D8%B8%D8%AA-%D8%A7%D8%B2-%DA%AF%D9%88%D8%B4%DB%8C-%D9%87%D8%A7%DB%8C-%D8%A7%D9%86%D8%AF%D8%B1%D9%88%DB%8C%D8%AF%DB%8C-%D8%AF%D8%B1-%D8%A8%D8%B1%D8%A7%D8%A8%D8%B1-%D8%AA%D9%87%D8%AF%DB%8C%D8%AF%D8%A7%D8%AA