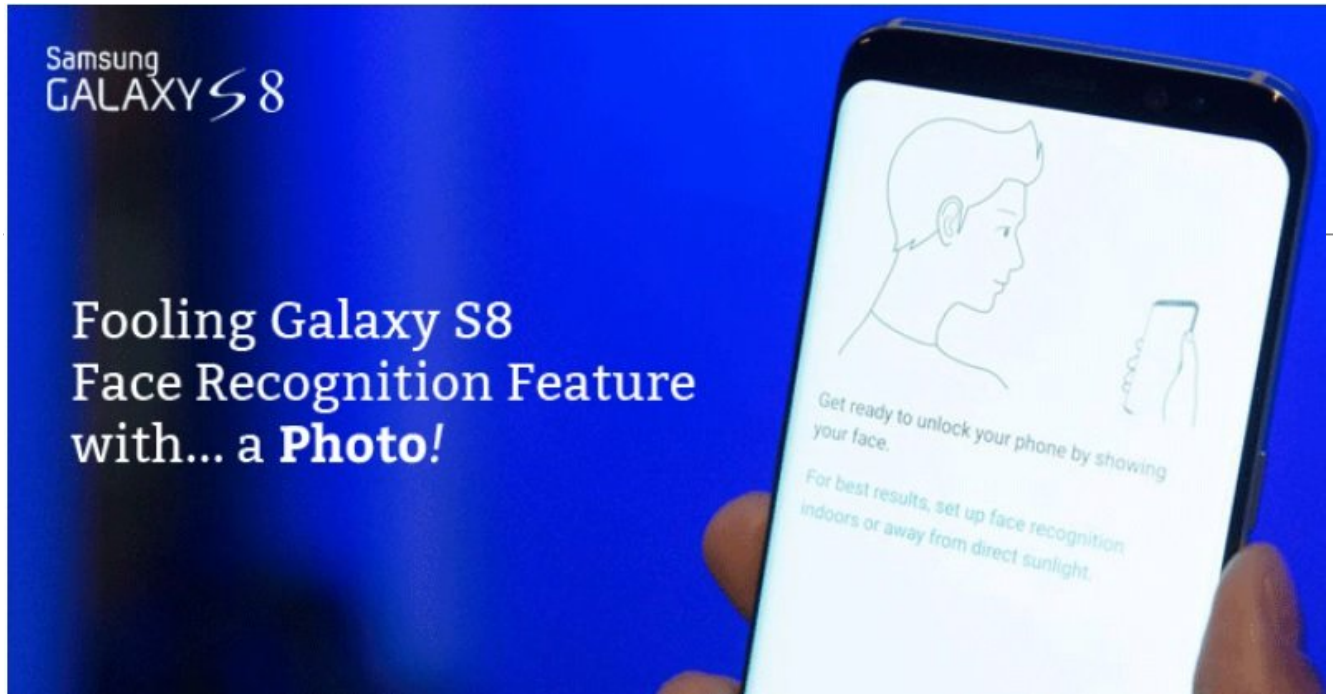
چالش‌های پرچم‌داران جدید

# مشکل امنیتی نگران‌کننده گوشی‌های گلکسی S8 و S8 Plus چیست و چگونه رفع می‌شود




سامسونگ به تازگی از دو گوشی جدید خود موسوم به گلکسی اس 8 و گلکسی اس 8 پلاس رونمایی کرده است. این شرکت امیدوار است با عرضه گوشی جدید خاطرات تلخ نوت 7 به دست فراموشی سپرده شود. اما به نظر می‌رسد این نیروهای تازه وارد در بدو ورود با یک مشکل امنیتی روبرو شده‌اند.

سامسونگ در جریان رویدادی که چهارشنبه هفته گذشته (Unpacked 2017) در نیویورک برگزار کرد، از دو پرچم‌دار خود رونمایی کرد. هر دو گوشی جدید مجهز به حسگر IRIS و ویژگی تشخیص چهره هستند. ویژگی جالب توجهی که به کاربران اجازه می‌دهد قفل گوشی هوشمند خود را از طریق الگوریتم تشخیص چهره باز کرده و به سایت‌های مختلف وارد شوند. در این سازوکار ورود کاربران باید گوشی هوشمند را درست به همان شکلی که یک عکس سلفی می‌گیرند مقابل چهره یا چشمان خود قرار دهند.

## مطلب پیشنهادی

احتمال معرفی نسخه مینی پرچمدار سامسونگ وجود دارد
**منتظر گلکسی اس 8 مینی 399 دلاری باشید!**

فناوری‌های بیومتریک از ویژگی‌های منحصر به فرد انسانی همچون عنبیه، اثرانگشت یا DNA برای شناسایی مردم استفاده می‌کنند و اکنون این ویژگی‌ها به منظور بهبود امنیت دستگاه‌های مصرفی با آن‌ها یکپارچه شده‌اند. اما امروزه شاهد این موضوع هستیم که هکرها با شناسایی رخنه‌هایی این دستگاه‌ها را مورد نفوذ قرار داده‌اند و به راحتی موفق شده‌اند به سامانه‌های امنیتی بیومتریک نفوذ کنند. اثرانگشت شاخص‌ترین تجربه تلخی بود که نشان داد نه تنها ساده‌تر از گذرواژه‌ها شکسته می‌شود بلکه در آینده نیز ممکن است دردسرهایی را برای صاحب اثرانگشت به وجود آورد. همچنین مشاهده کردیم که مکانیزم‌های اولیه تشخیص چهره نیز به راحتی قابل دور زدن هستند.

**مطلب پیشنهادی**

نگاهی نزدیک به پرچمداران سامی داشته باشید
**گلکسی اس 8 و اس 8 پلاس سامسونگ معرفی شدند + گالری عکس**

سامسونگ در دو گوشی جدید خود از حس‌گرهایی به منظور تشخیص چهره بهره برده است. اما سوال این است که این حس‌گرها تا چه اندازه ایمن هستند؟ گزارشی که به تازگی منتشر شده نشان می‌دهد که ظاهرا این حس‌گرها آن چنان که انتظار می‌رفت ایمن نیستند. ویدیویی که به تازگی منتشر شده نشان می‌دهد که این گوشی‌ها از طریق تصویری که به آن‌ها نشان داده می‌شود فریب می‌خورند. در ویدیویی که منتشر شده و روی یوتیوب قرار گرفته است، مالک دستگاه موفق شد از طریق تصویر خود حس‌گرهای تشخیص چهره مورد استفاده در گوشی‌های هوشمند سامسونگ را فریب داده و قفل آن‌را باز کند. این شکاف امنیتی نشان می‌دهد که هکرها به راحتی می‌توانند تصویر یک شخص را از شبکه‌های اجتماعی به دست آورده و به گوشی هوشمند مالک دستگاه وارد شوند.

البته کارشناسان امنیتی اعلام نکرده‌اند جزییات درون یک تصویر تا چه اندازه باید دقیق باشند تا بتوانند قفل دستگاه را باز کنند و همچنین تصویر باید در چه فاصله‌ای از گوشی هوشمند قرار بگیرد. نکته مهم دیگری که به درستی به آن پاسخ داده نشده این است که تصویر در چه زاویه‌ای از گوشی هوشمند باید قرار بگیرد. با همه این تفاسیر کاملا مشخص است که یک رخنه بزرگ امنیتی در مکانیزم تشخیص چهره حس‌گرهای سامسونگ وجود دارد.

موضوعی که بر نگرانی کارشناسان امنیتی افزوده در ارتباط با اخباری است که از مدت‌ها قبل منتشر شده و اعلام می‌دارد سامسونگ در چند ماه آینده به دنبال آن است تا از این مکانیزم برای پرداخت‌های الکترونیکی نیز استفاده کند. سامسونگ هنوز هیچ‌گونه واکنشی در ارتباط با این اخبار از خود نشان نداده اما کاملا مشخص است که از سامانه‌ای که هم اکنون در مرحله آزمایشی قرار دارد و ممکن است به آسیب‌پذیری‌هایی آلوده باشد، نمی‌توان در تراکنش‌های مالی استفاده کرد. البته مالکان این دستگاه‌ها برای ورود به دستگاه همراه خود می‌توانند از مکانیزم‌های دیگری همچون اثرانگشت یا گذرواژه‌ها برای ورود به دستگاه خود استفاده کنند.

**تاریخ انتشار:**

15 فروردین 1396

---

**نشانی منبع:** https://www.shabakeh-mag.com/security/7403