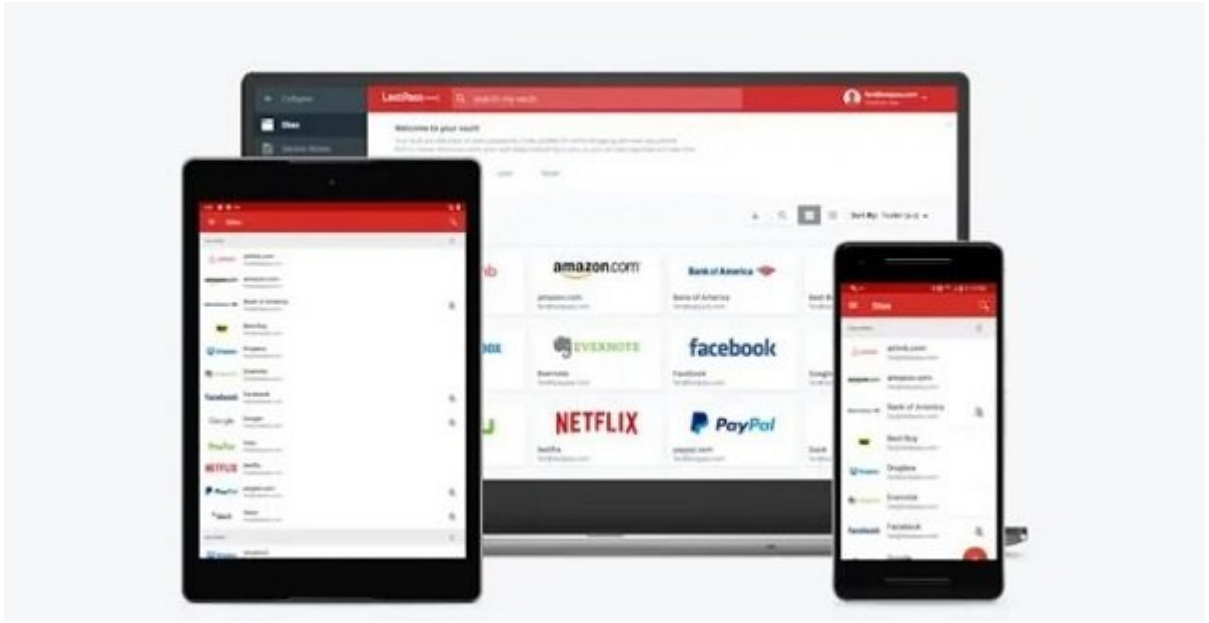
لزوم توجه به نکات پایه امنیت در سیستم‌عامل‌های همراه

10 نکته امنیتی برای محافظت از حریم خصوصی گوشی‌های اندرویدی

کاربران از گوشی‌های اندرویدی بیشتر از لپ‌تاپ‌ها استفاده می‌کنند، با این وجود در شرایطی که کاربران به خوبی نکات امنیتی لپ‌تاپ‌ها را رعایت می‌کنند، در مورد گوشی‌های اندرویدی چندان به مبحث امنیت توجهی ندارند و بیشتر آن‌ها یک جمله آشنا به زبان می‌آورند: «مگر فرد مهمی هستم که هکرها بخواهند گوشی اندرویدی من را هک کنند!» برخی دیگر نیز به دلیل این‌که تولیدکنندگان گوشی‌های همراه در بازه‌های زمانی مختلف وصله‌های امنیتی را برای اندروید ارائه می‌کنند نسبت به رعایت نکات امنیتی چندان حساس نیستند. هکرها از همین غفلت کاربران سوء استفاده می‌کنند تا روزنه‌ای در گوشی‌های اندرویدی برای دسترسی به اطلاعات حساس پیدا کنند. برای آن‌که از گزند هکرها در امان بمانید و شانس هکرها برای دسترسی به اطلاعات شخصی ذخیره شده روی گوشی را کم کنید لازم است به یکسری نکات امنیتی ساده و ابتدایی دقت کنید.

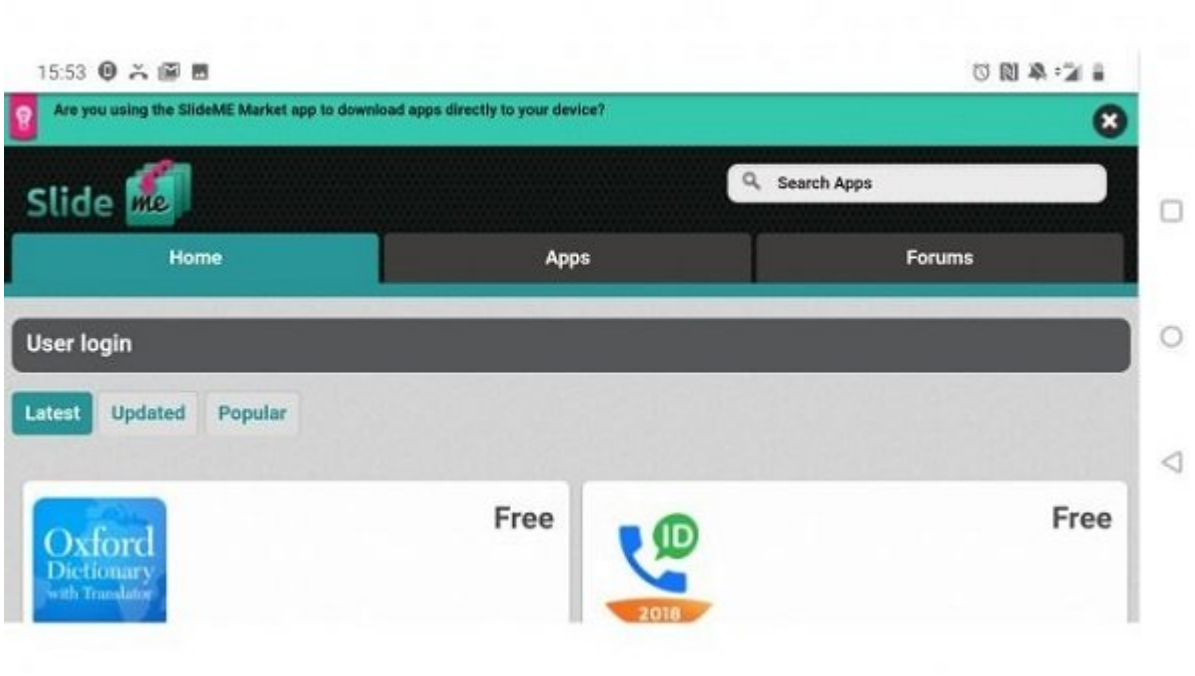
1. از یک برنامه مدیریت گذرواژه‌ها استفاده کنید



اگر از گذرواژه‌های قدیمی برای ورود به دستگاه‌های مختلف استفاده می‌کنید، نباید تعجب نکنید که ناگهان صدای عجیبی از یکی از وسایل هوشمند خانه همچون بلندگوی هوشمند یا گوشی همراه بلند شود و شما را غافل‌گیر کند. برخی از کاربران خود را محدود به یک گذرواژه ساده و قدیمی می‌کنند تا یادآوری آن ساده باشد و متاسفانه از این

گذرواژه برای ورود به دستگاه‌های مختلف استفاده می‌کنند. این‌کار واقعا دردسر آفرین است. یک برنامه مدیریت گذرواژه‌ها همچون Lastpass یک راهکار قدرتمند برای حل این مشکل است. نرم‌افزارهای مدیریت گذرواژه می‌توانند سایر گذرواژه‌ها را درون خود پنهان کنند و تنها یک گذرواژه اصلی در اختیارتان قرار دهند. برنامه‌های مدیریت گذرواژه می‌توانند گذرواژه‌هایی پیچیده و طولانی که به راحتی قابل حدس زدن نیستند را تولید کنند، بنابراین نیازی نیست به خود زحمت دهید تا یک گذرواژه پیچیده که شاید یک کلمه درون آن قرار دارد را انتخاب کنید. زمانی‌که یک برنامه مدیریت گذرواژه روی سیستم خود نصب کنید، در آینده هر زمان نیازمند پر کردن فیلدهایی باشید که اطلاعات حساس را طلب می‌کنند این برنامه‌ها به‌طور خودکار فیلدهای یاد شده را پر می‌کنند. برخی از کارشناسان امنیتی می‌گویند کاربران باید ویژگی پر کردن خودکار فیلدها روی گوشی و لپ‌تاپ خود را غیرفعال کنند، اما پیشنهاد می‌کنیم به جای این‌کار روی به‌کارگیری گذرواژه‌های قدرتمند و برنامه‌های مدیریت گذرواژه‌ها تمرکز کنید. از دیگر برنامه‌های قدرتمند در زمینه مدیریت گذرواژه‌ها می‌توان به 1Password ، Dashlane و Enpass اشاره کرد.

2. تا حد امکان از برنامه‌های جانبی فروشگاه‌های ثالث استفاده نکنید



انعطاف‌پذیری یکی از جذابیت‌های اندروید نسبت به iOS است، اما این انعطاف‌پذیری در برخی موارد باعث می‌شود ناخواسته به گوشی اندرویدی آسیب جدی وارد کنید. اندروید اجازه می‌دهد برنامه‌هایی که درون فایل‌های نصبی خام قرار دارند را نصب کنید، درست به همان شکلی که روی یک کامپیوتر دسکتاپی این‌کار را انجام می‌دهید. به عبارت ساده‌تر، فایل‌های برنامه که فرمت فایلی «apk» دارند را از فروشگاه‌های ثالثی همچون Getjar یا SlideMe بارگیری و روی گوشی نصب کنید.
کاربران زمانی که مشاهده می‌کنند برنامه‌ای روی فروشگاه گوگل‌پلی قرار ندارد یا به هر دلیل از فروشگاه گوگل‌پلی حذف شده است، آن‌را از فروشگاه‌های ثالث دانلود می‌کنند. متاسفانه، این ساده‌ترین راهکاری است که هکرها برای آلوده کردن گوشی‌های همراه از آن استفاده می‌کنند. برنامه‌هایی که درون فروشگاه‌های ثالث قرار می‌گیرند به لحاظ عاری بودن از وجود کدهای مخرب به درستی ارزیابی نمی‌شوند و ممکن است یک قطعه مخرب درون برنامه قرار گرفته باشد که دسترسی به سایر بخش‌های گوشی را برای یک هکر امکان‌پذیر می‌کند.

3. از 1234 به عنوان پین‌کد استفاده نکنید

استدلال‌های مختلفی در ارتباط با استفاده یا عدم استفاده از حس‌گر اثر انگشت به عنوان اصلی‌ترین مکانیزم امنیتی وجود دارد. برخی مدعی هستند که اثرانگشت به اندازه گذرواژه یا پین‌کد ایمن نیست و شما می‌توانید یک حس‌گر اثرانگشت را به سادگی شکست دهید. اگر قصد دارید از پین‌کدهای دیجیتالی روی گوشی خود استفاده کنید، نباید از یک پین‌کد ساده همچون 1111 یا 1234 استفاده کنید. در مورد قفل‌های الگوی تصویری نیز همین مسئله صادق است. اگر بیش از اندازه ساده باشند، قدرتمند نیستند. باید میان پیچیدگی و سهولت در تایپ و یادآوری تعادلی برقرار کنید تا هر زمان که نیاز داشتید با کمترین زحمت ممکن به گوشی دسترسی داشته باشید.

مطلب پیشنهادی

عکس‌برداری حرفه‌ای با بهترین کیفیت ممکن
12 ترفند جالب و کاربردی دوربین گوشی‌های اندرویدی

4. از وای‌فای عمومی برای انتقال داده‌های حساس استفاده نکنید

در شهرهای بزرگ، ارائه‌دهندگان خدمات اینترنتی اقدام به ارائه وای‌فای عمومی می‌کنند که به سختی می‌توان در مقابل دسترسی به یک انتخاب رایگان مقاومت کرد. بیشتر کارشناسان امنیتی توصیه می‌کنند برای حفظ امنیت بهتر است تحت هیچ شرایطی به وای‌فای عمومی متصل نشوید. در یک شبکه وای‌فای عمومی انواع مختلفی از حملات در کمین کاربران هستند تا داده‌های ذخیره شده در گوشی و اطلاعات مالی را به سرقت ببرند. یک هکر برای حمله به یک گوشی همراه از طریق یک وای‌فای عمومی به نبوغ چندان خاصی نیاز ندارد. اگر هنوز هم دوست دارید از وای‌فای عمومی برای وب‌گردی استفاده کنید، مطمئن شوید که از سایت‌هایی که با پروتکل https محافظت شده‌اند بازدید می‌کنید. تحت هیچ شرایطی جزئیات کارت اعتباری یا بانکی خود را با وای‌فای عمومی ارسال نکنید. ممکن است تمامی وب‌سایت‌های بانکی ایمن باشند، اما در یک شبکه وای‌فای عمومی این مکانیسم‌های امنیتی نمی‌تواند از شما در برابر حمله مرد میانی محافظت کنند.

مطلب پیشنهادی

ارتباط بهتر گوشی‌های اندرویدی با وای‌فای
15 تکنیک و ترفند جالب وای‌فای برای گوشی‌های اندرویدی

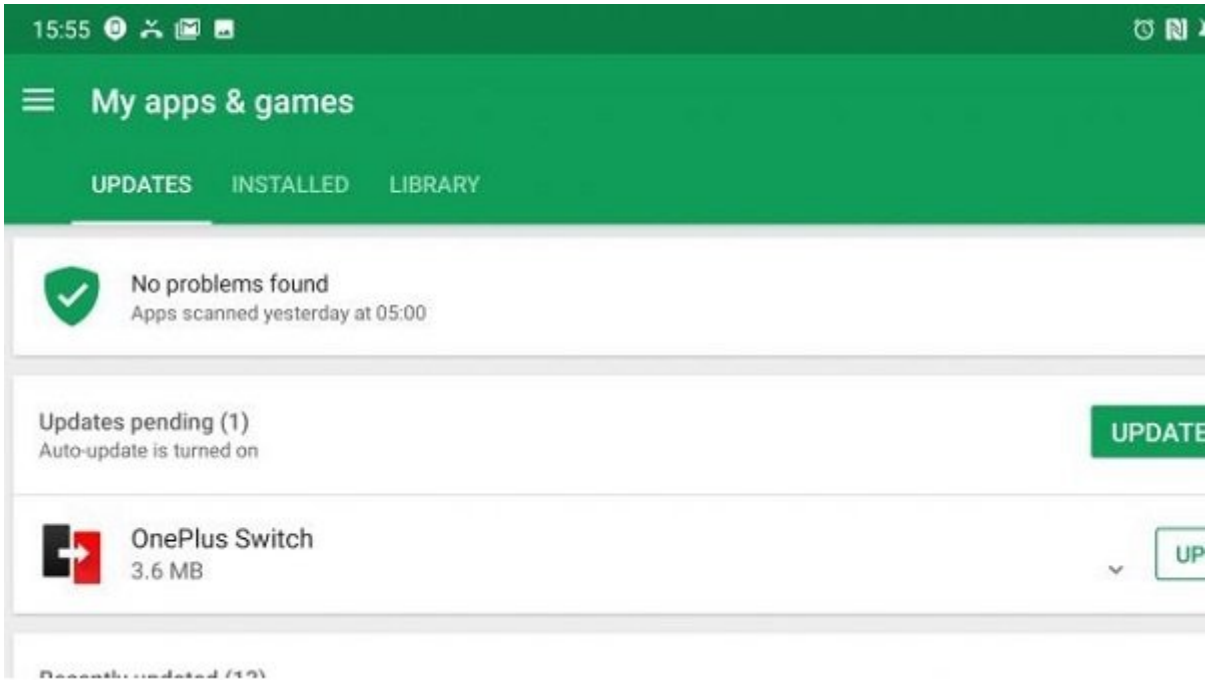
5- از یک شبکه خصوصی مجازی استفاده کنید

یک شبکه خصوصی مجازی در زمان ورود به اینترنت یک لایه محافظ اضافی پیرامون وب‌گردی قرار می‌دهد و تمامی اطلاعات ارسالی را میان گوشی و سرور مربوطه رمزگذاری می‌کند. عملکرد یک شبکه خصوصی مجازی ساده است. شبکه خصوصی مجازی به ویژه زمانی که قصد استفاده از یک وای‌فای عمومی را دارید از اطلاعات شخصی در برابر شنود محافظت می‌کند.

6. وصله‌های امنیتی را جدی بگیرید

نصب وصله‌های امنیتی ساده‌ترین و موثرترین راهکار مقابله با حملات هکری است. وصله‌های امنیتی، شکاف‌هایی که درون گوشی‌های هوشمند وجود دارند را پر می‌کنند و اجازه نمی‌دهند هکرها از آسیب‌پذیری‌های وصله نشده برای ضربه زدن به کاربران استفاده کنند. گوگل ماهیانه وصله‌های امنیتی را برای مقابله با تهدیدات و آسیب‌پذیری‌های شناسایی شده منتشر می‌کند. برای بررسی وصله‌هایی که ممکن است برای گوشی شما منتشر شده باشند به مسیر Settings > Security & Lock Screen > Security Update بروید. وصله‌های امنیتی ابتدا برای گوشی‌های پیکسل گوگل منتشر می‌شوند و در ادامه سایر تولیدکنندگان گوشی‌های همراه برای محصولاتی که خیلی قدیمی نیستند، وصله‌های امنیتی را منتشر می‌کنند.

7. برنامه‌های روی گوشی را به‌روز کنید



سیستم‌عامل گوشی تنها نرم‌افزاری نیست که باید به‌طور مرتب وصله‌ها را روی آن نصب کرد، برنامه‌های کاربردی نیز باید به‌روز شوند. یک رخنه امنیتی ساده در یک برنامه کاربردی به هکرها اجازه می‌دهد به یک گوشی اندرویدی وارد شده و انواع مختلفی از حملات را پیاده‌سازی کنند. برای بررسی به‌روزرسانی‌های منتشر شده برای یک برنامه کاربردی باید به گوگل پلی بروید و My Apps & Games و سپس زبانه Updates را انتخاب کنید. ویژگی به‌روزرسانی‌های خودکار (Auto updates) را روشن کنید و سعی نکنید نسخه‌های قدیمی از یک برنامه را روی گوشی خود نصب کنید. ویژگی Auto Update در مسیر Settings > update Apps قرار دارد.

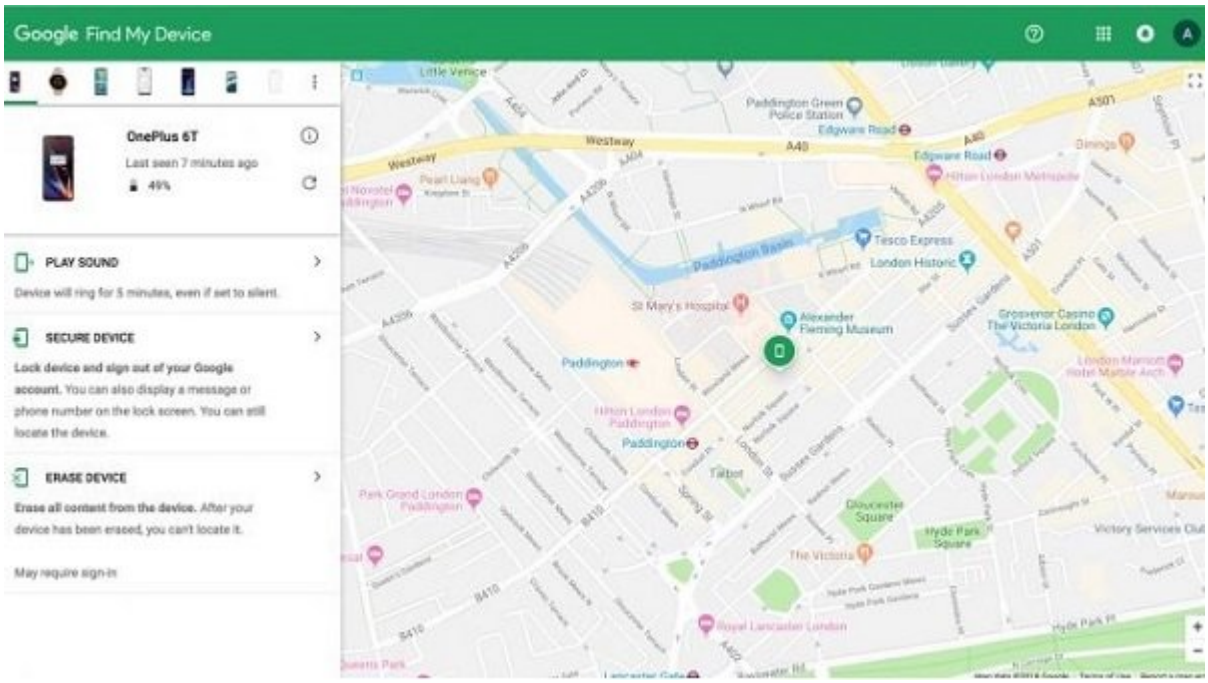
مطلب پیشنهادی

پنج اصل مهم در مدیریت حافظه گوشی‌های اندرویدی

8- احراز هویت دو مرحله‌ای را فعال کنید

بهترین راهکاری که برای مقابله با سرقت حساب کاربری گوگل در اختیارتان قرار دارد، مکانیزم احراز هویت دو مرحله‌ای است. با فعال کردن این ویژگی، هر زمان سعی کنید به حساب کاربری گوگل روی دستگاه دیگری وارد شوید، پین‌کدی برای گوشی شما ارسال می‌شود.
شاید فعال‌سازی این مکانیسم در ابتدا کمی خسته‌کننده و آزاردهنده باشد، اما امنیت را به‌طرز چشم‌گیری بهبود می‌بخشد. حتی اگر گذرواژه حساب کاربری در معرض خطر قرار گیرد، هکرها بازهم موفق نخواهند شد به اطلاعات شما دسترسی پیدا کنند. شما می‌توانید ویژگی احراز هویت دو مرحله‌ای گوگل را با مراجعه به وب‌سایت اختصاصی گوگل و ثبت‌نام در آن فعال کنید. در این حالت می‌توانید به گوگل اعلام دارید که یک کد تایید را از طریق سرویس پیام کوتاه برای گوشی شما ارسال کند یا از برنامه گوگل برای تایید ورود استفاده کنید.

9. قفل از راه دور را فعال کنید



به این نکته دقت کنید که احتمال سرقت یا گم شدن تلفن همراه در هر مکان و زمانی وجود دارد. اندروید قابلیت‌های منحصر به‌فردی در اختیار کاربران قرار می‌دهد تا زمان گم شدن یا به سرقت رفتن گوشی از داده‌های خود محافظت کنند. ویژگی Find My Phone به کاربر اجازه می‌دهد از طریق بلندگوی تلفن صدای هشداری پخش کند یا داده‌های روی گوشی را از راه دور پاک کند یا از حساب‌های کاربری خارج شده و گوشی را قفل کند. این ویژگی ممکن است در پیدا کردن گوشی کمک خیلی زیادی نکند؛ اما مانع از آن می‌شود تا اطلاعات هویتی شما به راحتی سرقت شوند.
برای آن‌که مطمئن شوید که قابلیت فوق به درستی کار می‌کند باید ویژگی دسترسی به موقعیت مکانی گوشی را فعال کنید. ویژگی فوق در بخش Security & Lock screen قرار دارد. در همین بخش ویژگی Find My Phone نیز وجود دارد.

مطلب پیشنهادی

اپ‌های دلخواه خود خود را در اندروید قفل کنید
چگونه در اندروید برای محافظت از اطلاعات شخصی، اپ‌ها را قفل کنیم

10. مراقب لینک‌های درون پیام‌های کوتاه باشید

بیشتر کاربران زمانی که پیام کوتاهی دریافت می‌کنند با اعتماد کامل به مخاطبی که پیام را برای آن‌ها ارسال کرده، پیوندی که درون پیام کوتاه قرار دارد را باز می‌کنند، غافل از آن‌که پیام ارسال شده ممکن است با هدف کلاه‌برداری ارسال شده باشد. نمونه‌های کلاسیک این پیام‌های کلاه‌بردارانه که حساب بانکی کاربر را نشان می‌روند از کاربر درخواست می‌کنند به حساب کاربری خود وارد شود و مشخصات خود را یکبار دیگر در صفحه جعلی به ظاهر متعلق به بانک وارد کند. در نمونه‌های جدیدتر یک پیام از طریق یک برنامه پیام‌رسان همچون واتس‌آپ برای کاربر ارسال می‌شود و درخواست می‌کند برای ادامه دسترسی به سرویس پیام‌رسان مبلغی را به شماره حسابی که تعیین شده واریز کند. زمانی‌که کاربر روی پیوند مربوطه کلیک می‌کند و جزییات حساب کاربری را درون فیلدهای مربوطه وارد می‌کند در حال وارد کردن اطلاعات درون یک صفحه بانکی جعلی است. بهترین راه برای مقابله با این کلاهبرداری‌ها نصب یک نرم‌افزار امنیتی یا فعال‌سازی یک گزینه امنیتی نیست، بلکه هوشیاری است. عقل سلیم می‌گوید به پیام‌های کوتاهی که از منابع ناشناس دریافت می‌کنید پاسخ ندهید و در صورت لزوم مراجع قانونی را مطلع کنید. البته برنامه‌هایی شبیه به Kaspersky Internet Security وجود دارند که تا حدودی از کاربران در برابر کلاه‌برداری‌های فیشینگ محافظت می‌کنند

تاریخ انتشار:

13 دی 1398

نشانی منبع:
https://www.shabakeh-mag.com/mobile-tricks/android-tricks/16429/10-%D9%86%DA%A9%D8%AA%D9%87-%D8%A7%D9%85%D9%86%DB%8C%D8%AA%DB%8C-%D8%A8%D8%B1%D8%A7%DB%8C-%D9%85%D8%AD%D8%A7%D9%81%D8%B8%D8%AA-%D8%A7%D8%B2-%D8%AD%D8%B1%DB%8C%D9%85-%D8%AE%D8%B5%D9%88%D8%B5%DB%8C-%DA%AF%D9%88%D8%B4%DB%8C%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