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

در حالی که تولیدکنندگان بزرگ گوشی‌های هوشمند در تلاش هستند تا این ابزارها را به شکل ایمنی در اختیار مصرف‌کننده نهایی قرار دهند، در این میان کاربران نیز باید به مسئولیت‌هایی که در این زمینه دارند، متعهد باشند. اگر کاربران نسبت به این انجام یکسری کارها احساس مسئولیت کنند آن‌گاه با خیال آسوده می‌توانند از گوشی‌های هوشمند خود استفاده کرده و راه دسترسی به داده‌های شخصی را به روی افراد غیرمجاز ببندند.

قسمت اول این مقاله را می‌توانید در اینجا ببینید.

6. از شبکه‌های وای‌فای ایمن استفاده کنید

به‌کارگیری وای‌فای عمومی و رایگان برای اغلب کاربران وسوسه‌انگیز است. اما نکته‌ای که باید به آن توجه داشته باشید این است که این شبکه‌ها در اغلب موارد ایمن نبوده و ممکن است دامی باشد که هکرها برای شما ترتیب داده‌اند. به‌طوری که اطلاعات شخصی و اطلاعات مربوط به کارت‌های بانکی را به سرقت ببرند. در اغلب موارد هکرها از طریق ساخت هات‌اسپات‌های جعلی به راحتی موفق می‌شوند کاربران را فریب دهند. به همین دلیل پیشنهاد ما این است که تا حد امکان از چنین شبکه‌هایی استفاده نکنید. همچنین اگر مجبور شدید از این شبکه‌ها برای ورود به اینترنت و دسترسی به حساب‌های کاربری خود استفاده کنید، سعی کنید از حالت InPrivate mode که درون مرورگرها قرار داشته و در زمان خروج از یک سایت اطلاعات را پاک می‌کنند استفاده کنید. اما سعی نکنید از طریق شبکه‌های وای‌فای عمومی به حساب‌های بانکی متصل شده یا تراکنش‌های مالی انجام دهید.

7. از برنامه‌های مدیریت گذرواژه‌ها استفاده کنید

زمانی که صحبت از گذرواژه‌ها به میان می‌آید شما چند گزینه پیش رو دارید. اول آن‌که برای همه حساب‌های کاربری خود از یک گذرواژه یکسان استفاده کنید که در عمل راهکار عاقلانه‌ای نیست. دوم آن‌که گذرواژه‌های به کار گرفته شده را روی برگه‌ای یادداشت کنید که ایده خوبی است اما احتمال این‌که برگه یادداشت را گم کرده یا سایرین آن‌را مشاهده کنند وجود دارد. راهکار سومی که پیش روی شما قرار دارد این است که گذرواژه‌ها را حفظ کنید که این‌کار برای اغلب کاربران شدنی نیست. اما راهکار چهارمی که قدرت بیشتری در اختیار شما قرار می‌دهد به‌کارگیری برنامه‌های مدیریت گذرواژه‌ها است. گوگل نیز در این زمینه سرویس‌هایی ارائه می‌کند، اما اغلب کاربران تمایلی ندارند گذرواژه‌های خود را در اختیار گوگل قرار دهند. در نتیجه به سراغ برنامه‌هایی می‌روند که به آن‌ها اجازه می‌دهد گذرواژه‌های متعدد به کارگرفته شده برای حساب‌های کاربری را در این برنامه وارد کرده، اما در مقابل تنها یک گذرواژه اصلی را حفظ کنند. برنامه‌هایی همچون LastPass، 1Password و Dashlane از جمله برنامه‌های معروف و قدرتمندی هستند که پیش روی شما قرار دارد.

8. از یک ضد بدافزار استفاده کنید

درست است که گوگل پلی به خوبی می‌تواند از گوشی شما محافظت به عمل آورد، اما برای در امان ماندن از گزند بدافزارها راهکار عاقلانه‌ای است که از یک ضدویروس قدرتمند در این زمینه استفاده کنید. در میان ضدبدافزارهای رایجی که امروزه در اختیار کاربران اندرویدی قرار دارد Avast Mobile Security & Antivirus یکی از بهترین‌ها است. ضدویروسی که عملکرد خوبی داشته و امکانات متنوعی در اختیارتان قرار می‌دهد. بسته امنیتی قدرتمند دیگری که در اختیارتان قرار دارد Norton Mobile Security است که البته برای دستیابی به قابلیت‌های بیشتر آن باید هزینه مربوطه را پرداخت کنید.

9. در موارد غیرضروری گزینه‌های ارتباطی و اتصال به گوشی خود را خاموش کنید

اگر از وای‌فای یا بلوتوث استفاده نمی‌کنید، بهتر است آن‌ها را خاموش کنید. بزرگ‌ترین مزیت این‌کار طولانی شدن عمر باتری دستگاه است. همچنین به این موضوع توجه داشته باشید که با توجه به رخنه‌های امنیتی شناسایی شده در مکانیزم بلوتوث این امکان وجود دارد که هکرها بتوانند از طریق بلوتوث به گوشی اندرویدی شما حمله کنند.

10. در صورت عدم استفاده از یک برنامه کاربردی آن‌را پاک کنید

هر برنامه کاربردی آسیب‌پذیری‌های خاص خود را دارد. اغلب برنامه‌های کاربردی اندروید به شکل مرتب به‌روزرسانی‌هایی را دریافت می‌کنند تا آسیب‌پذیری‌های شناسایی شده را ترمیم کنند، اما در این میان برنامه‌هایی هم وجود دارند که هیچ‌گاه به‌روزرسانی‌ها را دریافت نمی‌کنند. به همین دلیل توصیه ما به شما این است که در صورت عدم استفاده از برنامه‌های کاربردی آن‌ها را از روی گوشی خود پاک کنید. هر چه تعداد برنامه‌های کاربردی روی گوشی شما کم باشد به همان نسبت احتمال وجود آسیب‌پذیری و نفوذ به گوشی شما به حداقل می‌رسد.

چگونه گذرواژه قدرتمندی را انتخاب کنیم؟

همان‌گونه که در بخش اول این مطلب به آن اشاره کردیم به‌کارگیری گذرواژه‌ها هنوز هم یکی از ایده‌آل‌ترین مکانیزم‌هایی است که پیش روی شما قرار دارد. اما برای دستیابی به این مکانیزم امنیتی باید به یکسری اصول توجه داشته باشید. ما در این مقاله به تعدادی از این اصول اشاره خواهیم کرد.

گذرواژه‌های طولانی انتخاب کنید

یک گذرواژه ایده‌آل در حالت استاندارد باید حداقل 12 و حداکثر 15 کاراکتر داشته باشد. مارک برنت، نویسنده کتاب Perfect Passwords در این خصوص گفته است: «گذرواژه‌های شما ضمن آن‌که باید پیچیده باشند، باید اندازه طولانی نیز داشته باشند. اگر شما از یک گذرواژه طولانی که تنها از حروف کوچک ساخته شده استفاده کنید به مراتب ایمن‌تر از گذرواژه کوتاهی است که از حروف بزرگ و کوچک و اعداد ساخته شده است. به جای آن‌که روی انتخاب کاراکترهای خاص و عجیب متمرکز شوید، بهتر است از عبارات و کلماتی که یادآوری آن‌ها برای شما ساده بوده اما به راحتی قابل حدس زدن نیستند استفاده کنید.»

2. گذرواژه‌های عجیب و غریب را انتخاب کنید

گذرواژه‌هایی که از سوی افراد مختلف انتخاب می‌شود بیان‌گر این موضوع هستند که این گذرواژه‌ها ایمن نیستند. مورگان اسلین مدیر SplashData در این خصوص گفته است: «ما همواره گذرواژه‌های طولانی را پیشنهاد می‌کنیم، اما این حرف به معنای آن نیست که شما در یک گذرواژه از کاراکترهای تکراری استفاده کنید. تا حد امکان سعی کنید از گذرواژه‌هایی که به اسامی افراد مشهور اشاره دارند استفاده نکنید. در سال گذشته میلادی (2017) اغلب کاربران از عبارت Star wars به عنوان گذرواژه خود استفاده کرده بودند. همواره به دنبال انتخاب گذرواژه‌های ترکیبی باشید که متشکل از کاراکترها و اعداد هستند.»

3. از کاراکترهای خاص به شکل صحیحی استفاده کنید

بهترین حالتی که در این زمینه پیشنهاد می‌شود این است که اعداد، کاراکترهای خاص و سمبل‌ها را به جای آن‌که در اول یا آخر گذرواژه قرار دهید در وسط گذرواژه به کار ببرید. لوری فیث کرانور متخصص رمزنگاری و استاند دانشگاه کارنگی ملون در این خصوص می‌گوید: «بررسی‌های ما نشان می‌دهد که مردم در اغلب موارد حروف بزرگ را در ابتدای گذرواژه و کاراکترهای خاص یا اعداد را در آخر گذرواژه قرار می‌دهند. اما پیشنهاد ما این است که کاراکترهای خاص را در وسط گذرواژه استفاده کنید تا حدس زدن آن برای هکرها و برنامه‌ها رمزشکن سخت شود. »

4. از یک ترکیب در دو مکان استفاده نکنید

اگر گذرواژه قدرتمندی را انتخاب کرده‌اید، اما در مقابل از این گذرواژه در همه سایت‌ها استفاده کرده‌اید در عمل خود را در معرض یک خطر بزرگ قرار داده‌اید. اگر شما در گذرواژه خود از کاراکترهایی همچون @%&#@ استفاده کنید در عمل کار را برای هکرها سخت کرده‌اید، اما این حرف به معنای آن نیست که از این گذرواژه در ارتباط با حساب‌های کاربری مختلف استفاده کنید. جو سیگریست، کارشناس امنیتی شرکت LastPass در این خصوص می‌گوید: «اگر از یک گذرواژه قدرتمند برای همه حساب‌های کاربری خود در سایت‌های مختلف استفاده کنید و هکری موفق شود یکی از این سایت‌ها را شکسته و به بانک‌اطلاعاتی آن سایت یا سرویس دست پیدا کند در عمل دسترسی به همه حساب‌های کاربری شما را به دست خواهد آورد. شما همواره باید از گذرواژه‌های منحصر به فرد برای هر سایت یا سرویسی استفاده کنید.»

5. گذرواژه‌های خود را در بازه زمانی مشخص تغییر دهید

کاربران در این زمینه به دو گروه تقسیم می‌شوند. گروه اول کاربرانی هستند که هیچ‌گاه گذرواژه حساب خود را تغییر نمی‌دهند و در عمل راه را برای ورود هکرها هموار می‌سازند. گروه دوم کاربرانی هستید که در فواصل زمانی بسیار کوتاه گذرواژه خود را تعویض می‌کنند اما در عمل در هر مرتبه تنها یک یا دو کاراکتر به گذرواژه قبلی خود اضافه می‌کنند. با این وجود ضرورتی ندارد گذرواژه خود را هر دو هفته یکبار تعویض کنید. به جای تعویض مرتب گذرواژه‌ها سعی کنید از گذرواژه‌هایی با طول زیاد استفاده کنید.

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

15 آذر 1398

نشانی منبع:
https://www.shabakeh-mag.com/tricks/mobile-tricks/16326/%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