ترفندهایی کلیدی برای محافظت از اطلاعات گوشی در برابر هکرها

چگونه از گوشی اندرویدی خود در برابر هکرها و خرابکارها محافظت کنیم؟

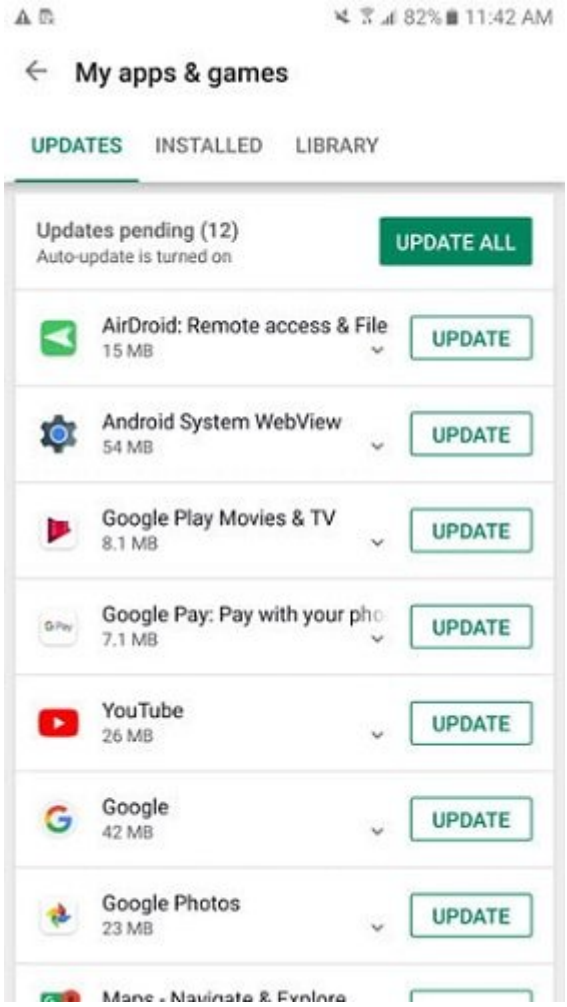
گوشی که در دست دارید از تمام رازهای شما باخبر است. با استفاده از این نکات کاربردی گوشی خود را از شر هکرها و خرابکارها در امان نگه دارید.

وقتی **گوشی** هک می‌شود درست مثل این است که از خانه شما دزدی شده است. هک **گوشی** بدترین نوع حمله به حریم شخصی و تعرض به فضای شخصی شما است و مدت زمان زیادی طول می‌کشد تا متوجه شوید که چه چیزهایی گم شده است. **گوشی** فقط اطلاعات باارزش شما را نگه نمی‌دارد، بلکه به مهاجمان خبر می‌دهد که کدام بخش از این اطلاعات بیشترین اهمیت را برای شما دارند.

گوشیها همیشه هدف حمله **هکر**ها و مجرمان هستند. برای اینکه از **گوشی** و محتویات روی آن در برابر چشمان و

انگشتان مهاجمان مراقبت کنید باید استراتژی خاصی را برای محافظت از این اطلاعات ارزشمند به‌کار بگیرید. در زیر نکاتی را به‌شما آموزش می‌دهیم که با استفاده از آنها می‌توانید **گوشی اندرویدی** خود را در برابر حملات **هکرها** و خرابکارها محافظت کنید.

سیستم‌عامل و اپ‌های گوشی خود را به‌روزرسانی کنید

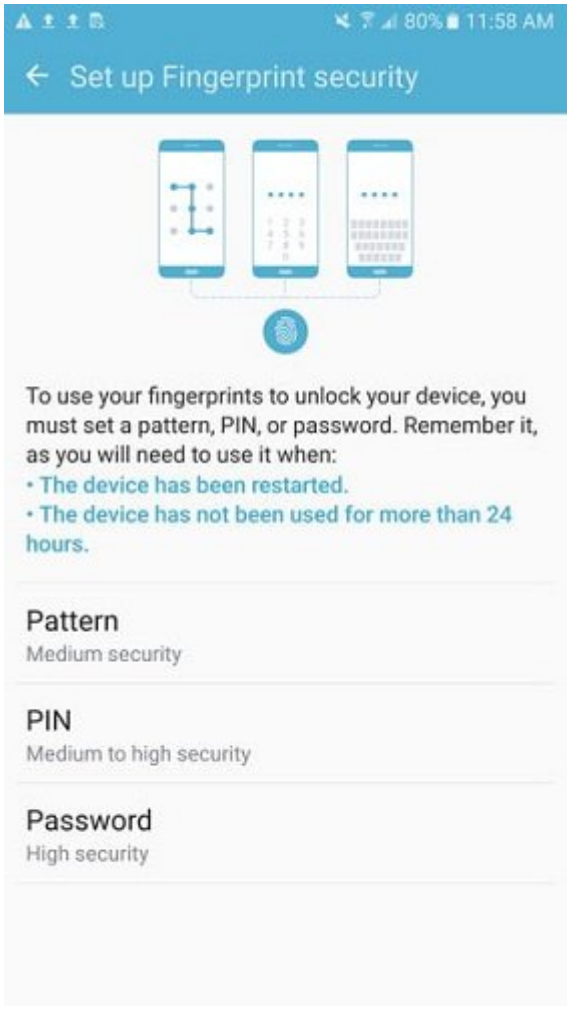


شرکت‌های نرم‌افزاری دائما در حال به‌روزرسانی محصولات نرم‌افزاری خود هستند. بسیاری از به‌روزرسانی‌های نرم‌افزار و وصله‌هایی که برای ترمیم باگ‌ها منتشر می‌شوند باعث بهبود امنیت و بالا بردن سپر دفاعی **گوشی** در برابر سارقان و متجاوزان می‌شوند. هر زمان که خبر تازه‌ای در خصوص به‌روزرسانی سیستم‌عامل یا هر اپلیکیشنی که استفاده می‌کنید منتشر شد، بدون تأخیر آنها را نصب کنید.

از وای‌فای عمومی دوری کنید

تقریبا همه کاربران از خطرات استفاده از وای‌فای عمومی و باز مطلع هستند. وای‌فای عمومی رایگان که در تمام مراکز خرید، کافه‌ها، رستوران‌ها، فرودگاه‌ها و سایر اماکن عمومی ارائه می‌شود بهترین فرصت برای سوءاستفاده **هکر**ها است. سعی کنید حتی‌الامکان از اینترنت خط خود استفاده کنید و هروقت در مکان‌های عمومی هستید وای‌فای **گوشی** را خاموش کنید. علاوه بر این، در مکان‌های عمومی بلوتوث **گوشی** را هم خاموش کنید، مگر اینکه اسمارت‌واچی داشته باشید که برای ارتباط نیاز به بلوتوث دارد.

گوشی خود را قفل کنید

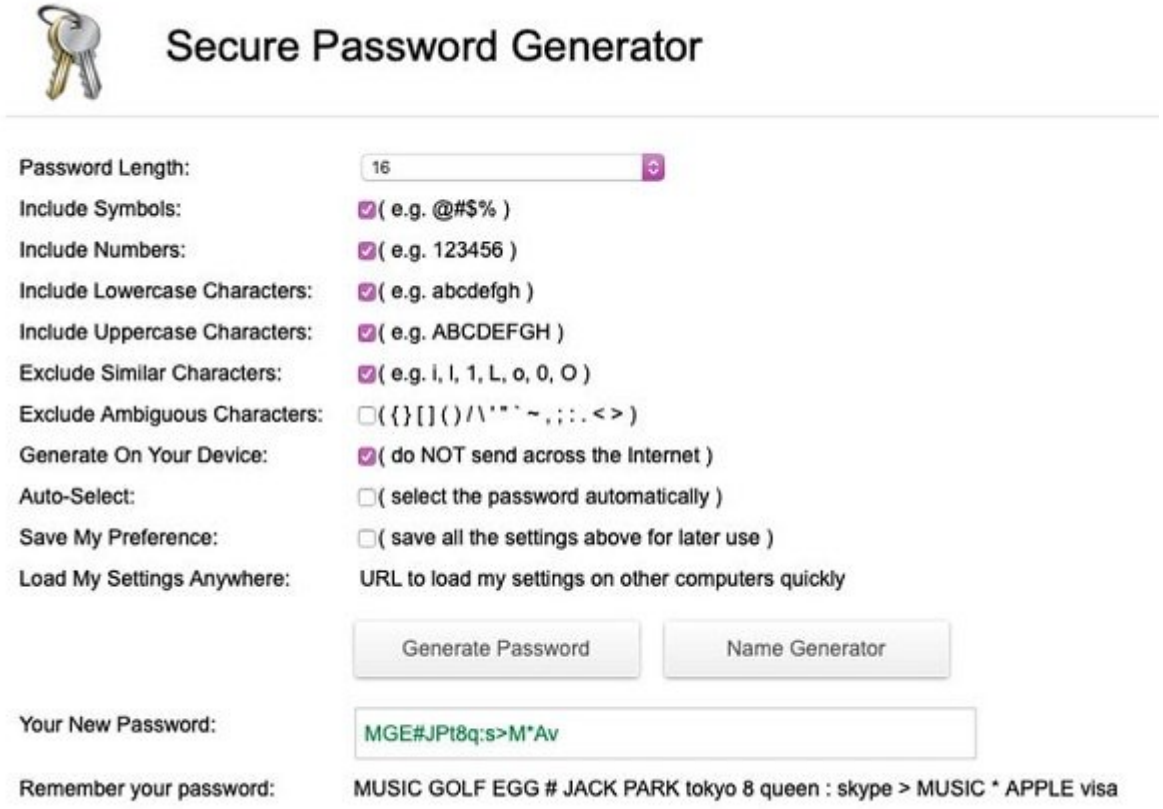


همیشه برای باز کردن **گوشی** از کد عبور چهار یا شش رقمی استفاده کنید. شاید اینکه همیشه برای کار با **گوشی** نیاز به وارد کردن کد عبور داشته باشید چندان خوشایند نباشد، اما این سناریو را به‌یاد داشته باشید که اگر روزی بر حسب اتفاق **گوشی** شما گم شود، هر کسی می‌تواند از داستان زندگی شما مانند ایمیل‌ها، مخاطبان، عکس‌ها و اطلاعات بانکی خبردار شود. حالا اگر این کد عبور تلفیقی از حروف و اعداد باشد امکان نفوذ بسیار کم می‌شود. طرفدار کد عبور نیستید؟ نگران نباشید. با وجود حسگرهای اثر انگشت و هم‌چنین تشخیص چهره می‌توانید به‌سادگی و به‌سرعت وارد **گوشی** خود شوید.

از احراز هویت دو مرحله‌ای استفاده کنید

احراز هویت دو مرحله‌ای هم از آن دسته روش‌هایی است که معمولا مورد بی‌توجهی قرار می‌گیرد. چراکه باید یک مرحله بیشتر برای ورود به **گوشی** را پشت سر بگذارید. اما با استفاده از آن، یک لایه امنیتی بیشتر به **گوشی اندرویدی** خود اضافه می‌کنید.

از کلمات عبور قوی استفاده کنید



کلمه عبوری که برای **گوشی** انتخاب می‌کنید بهتر است حاوی 16 تا 20 کاراکتر شامل حروف، اعداد، علایم باشد. هم‌چنین کوچکی و بزرگی هم برای حروف درنظر بگیرید. افرادی که با استفاده از بروت فورس کلمات عبور را کرک می‌کنند قادر هستند تا در خیلی از موارد کلمات عبور قوی را هم بشکنند. اما ساده کردن کار **هکر**ها با به‌کارگیری تاریخ تولد، نام حیوان خانگی یا هر چیزی شبیه به این موارد به‌عنوان کلمه عبور ایده بسیار هولناکی است.

تولیدکننده‌های آنلاین زیادی هستند که کلمات عبور امن تولید می‌کنند. بهتر است هر شش ماه یک بار کلمات عبور خود را عوض کنید یا اگر اخباری در خصوص هک شدن یک برنامه خاص شنیدید خیلی سریع کلمه عبور خود را تغییر دهید. اما یک نکته مهم دیگر: پرسش‌های امنیتی را با جواب‌های درست پاسخ ندهید. برای هر حالت یک‌سری جواب مختلف داشته باشید.

مراقب ایمیل‌های اسپم و فیشینگ باشید

یکی از راه‌های ساده برای **هکر**ها نفوذ به **گوشی** از طریق صندوق پست الکترونیک است. ایمیل‌های فیشینگ به‌گونه‌ای طراحی می‌شوند که که با فریب شما امکان دسترسی به اکانت را فراهم می‌کنند. از کلیک بر روی ایمیل‌های تبلیغاتی، باز کردن پیوست‌های مشکوک یا اجرای به‌روزرسانی‌های اپی که از طریق ایمیل یا پیامک تبلیغ می‌شوند خودداری کنید.

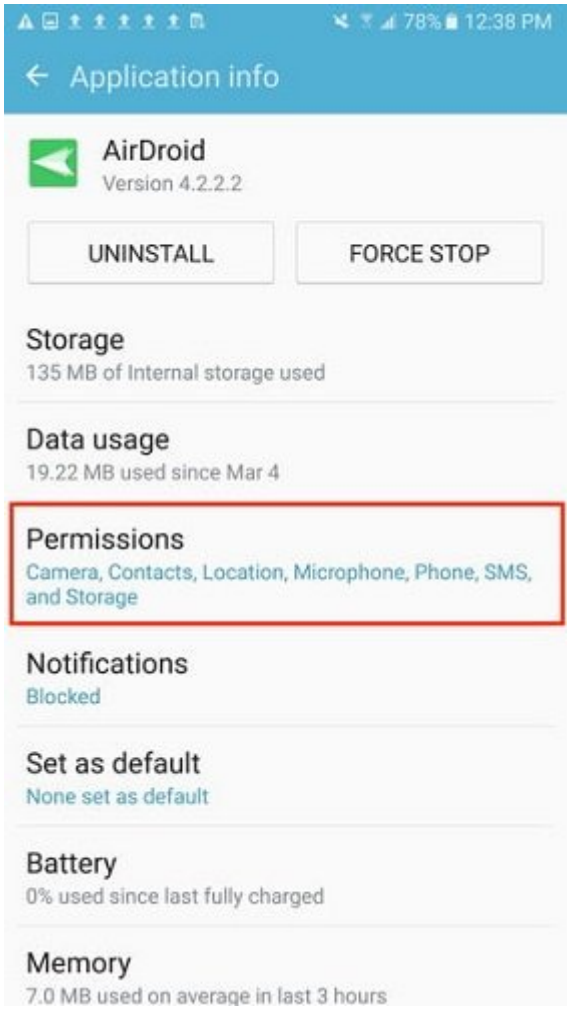
از خصوصیات محافظتی از پیش ساخته شده داخل دستگاه استفاده کنید

اگر **گوشی** شما به‌هر دلیلی گم شد یا به‌سرقت رفت می‌توانید با ویژگی‌هایی مانند Find My Phone و هم‌چنین Dind My Device برای اندروید سعی کنید تا محل فعلی **گوشی** سرقتی را روی نقشه پیدا کنید. حتی اگر **گوشی** را در خانه یا محل کار گم کردید با این سرویس‌ها می‌توانید گوشی را وادار به زنگ زدن کنید. علاوه بر اینها، می‌توانید **گوشی** را طوری تنظیم کنید که اگر کدعبور چندین بار اشتباه وارد شد تمام اطلاعات روی **گوشی** پاک شود.

از آنتی‌ویروس استفاده کنید

هکرها بدافزارهایی که کلمات عبور و اطلاعات اکانت را سرقت می‌کنند دوست دارند. می‌توانید با یک اپ آنتی‌ویروس مانند آواست، مک‌آفی و پاندا با اینگونه موارد مبارزه کنید.

مجوزهای اپ را مدیریت کنید



مجوزهای اپ‌ها را بررسی کنید. می‌توانید دسترسی به دوربین، میکروفون، لیست مخاطبان یا لوکیشن توسط اپ‌ها را متوقف کنید. مجوزهای داده شده به اپ‌را زیرنظر داشته باشید و مواردی که مورد نیاز نیستند را حذف کنید. برای آیفون به مسیر Settings > Privacy بروید. در این قسمت لیست کاملی از تمام اپ‌ها و مجوزهای آنها را می‌بینید. در مورد **اندروید**، این آدرس برای دستگاه‌های مختلف فرق می‌کند. اما روی گوشی گوگل پیکسل می‌توانید به مسیر Settings > Apps & notifications > Advanced > Permission manager و روی گوشی سامسونگ گلکسی به مسیر Settings > Apps > App permissions بروید.

بکاپ

همیشه باید آماده بدترین حالت‌ها باشید. از تمام فایل‌ها و تصاویر مهم خود بکاپ داشته باشید.

بدانید که اپ‌ها از کجا می‌آیند

فقط اقدام به دانلود اپ‌های قدیمی نکنید. در حالی‌که دانلود اپ‌های آیفون تنها به اپل اپ استور محدود است، منابع متعددی به‌غیر از گوگل پلی استور برای دانلود برنامه‌های **اندروید**ی وجود دارد. بهترین راه برای دوری کردن از بدافزارها روی **اندروید** انتخاب آنها از گوگل پلی استور است. هیچ‌وقت اپ‌ها را از طریق پیامک‌هایی که دریافت می‌کنید نصب نکنید.

از شارژرهای عمومی استفاده نکنید

برای شارژ **گوشی** خود فقط از پورت‌های USB قابل اعتماد مانند کامپیوتر یا خودروی خود استفاده کنید. **هکر**ها می‌توانند پورت‌های شارژ USB که در اماکن عمومی مانند فرودگاه‌ها قرار دارد را هک کنند. در هنگام سفر علاوه بر کابل USB دوشاخه مربوط به آن‌را هم همراه داشته باشید. **هکر**ها نمی‌توانند از طریق آداپتر USB شخصی شما به اطلاعاتی که روی **گوشی** دارید دسترسی پیدا کنند.

منبع:

دیجیتال ترندز

تاریخ انتشار:
14 مرداد 1398

نشانی منبع:
https://www.shabakeh-mag.com/tricks/15784/%DA%86%DA%AF%D9%88%D9%86%D9%87-%D8%

A7%D8%B2-%DA%AF%D9%88%D8%B4%DB%8C-
%D8%A7%D9%86%D8%AF%D8%B1%D9%88%DB%8C%D8%AF%DB%8C-
%D8%AE%D9%88%D8%AF-%D8%AF%D8%B1-%D8%A8%D8%B1%D8%A7%D8%A8%D8%B1-
%D9%87%DA%A9%D8%B1%D9%87%D8%A7-%D9%88-
%D8%AE%D8%B1%D8%A7%D8%A8%DA%A9%D8%A7%D8%B1%D9%87%D8%A7-
%D9%85%D8%AD%D8%A7%D9%81%D8%B8%D8%AA-
%DA%A9%D9%86%DB%8C%D9%85%D8%9F