همیشه مراقب هک شدن گوشی خود باشید

از کجا بفمیم که گوشی ما هک شده است؟

بدون شک تلفن‌های همراه تبدیل به بخش مهمی از زندگی ما شده‌اند. علاوه بر این، تلفن همراه ابزاری شده که هر روز آن را داخل جیب یا کیف خود گذاشته و به نقاط مختلف حمل می‌کنیم. برای همین همیشه داده‌های ما در معرض خطر سارقان و هکرها هستند. بنابراین، ضروری است که نکات ایمنی را در این خصوص رعایت کنیم.

هکرها دائما در حال تیز کردن ابزار خود هستند. اما در اینجا به شما آموزش می‌دهیم که چگونه متوجه شوید **گوشی** شما **هک** شده و چگونه خود را در برابر **هک گوشی محافظت** کنید.

گوشی شما چگونه ممکن است هک شود

چندین روش برای **هک گوشی** وجود دارد. بعضی از این روش‌ها اصلا نیازی به دانش پیشرفته فناوری هم ندارند:

1- حمله جابجایی سیم کارت

هکرها با این روش حمله شماره تلفن شما را به سیم کارت خودشان انتقال می‌دهند و کنترل اکانت شما را به دست می‌گیرند.

2- جاسوس‌افزار

جاسوس‌افزارها می‌توانند داده‌های شما را گردآوری کنند. برخی از اپ‌های جاسوسی به‌قدری ساده هستند که هر شخصی بدون داشتن دانش پیشرفته در حوزه فناوری هم می‌تواند از آنها استفاده کند. **هکر**ها با استفاده از **جاسوس‌افزار**ها از راه دور تمام فعالیت‌های **گوشی** شما را رصد می‌کنند. اگر کسی چنین اپی را نصب کند می‌تواند به دستگاه شما دسترسی مستقیم پیدا کند.

3- بدافزار

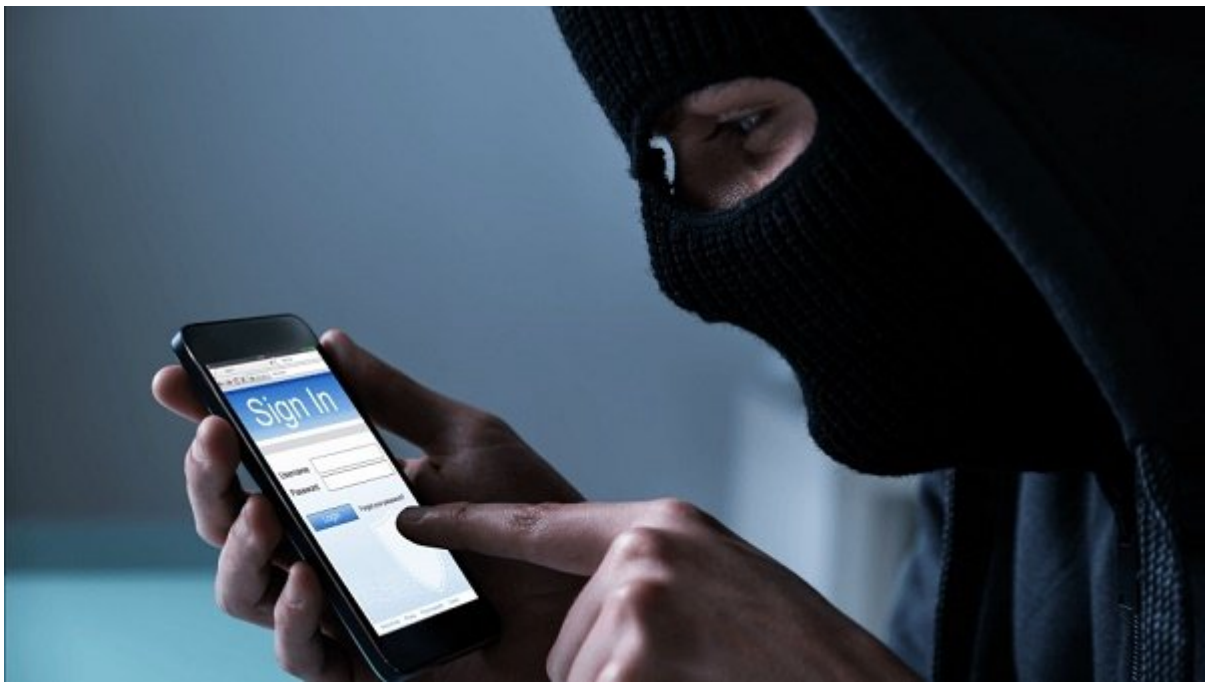
استفاده از شبکه‌های وای‌فای عمومی هم می‌تواند باعث شود تا **گوشی** شما به نرم‌افزارهای مخرب یا **بدافزار**ها آلوده شود. **هکر**ها این توانایی را دارند تا با برپایی شبکه‌های وای‌فای ساختگی و جعلی **گوشی** شما را به سمت سایت‌های فیشینگ منحرف کنند یا از طریق کابل USB در ایستگاه‌های مخصوص شارژ **گوشی** کنترل **گوشی** شما را به دست بگیرند.

4- پیام‌های فیشینگ

ایمیل‌ها، متن‌ها و پیام‌های فیسبوک که حاوی لینک‌های خراب‌کارانه باشند می‌توانند روی **گوشی بدافزار** نصب کرده و اطلاعات شما را به‌سرقت ببرند.

5- دانلود بدافزار

حتی ممکن است وقتی در حال دانلود اپ از سایت‌های مشکوک هستید یا با کلیک بر روی لینک‌ها یا پاپ‌آپ‌های غیرقابل اعتماد اقدام به دانلود **بدافزار** بر روی **گوشی** خود کنید.



چگونه بفهمیم که گوشی ما هک شده است

آیا تا به‌حال این سئوال را از خود پرسیده‌اید که: "آیا **گوشی** من **هک** شده است؟" با درنظر گرفتن موارد زیر می‌توانید از این قضیه مطمئن شوید:

1- زمانی‌که روی **گوشی** متوجه چیزی می‌شوید که اصلا آن را نمی‌شناسید (مانند اپ‌ها، پیام‌هایی که ارسال نکرده‌اید، خریدهایی که انجام نداده‌اید، یا تماس‌های تلفنی مشکوک)

2- **گوشی** شما کند شده است. ممکن است **گوشی** در حال استفاده بیش از اندازه از منابع باشد، باتری زود تمام شود و نسبت به حالت معمول داغ‌تر شود. برخی از فعالیت‌های **هکر**ها می‌تواند قدرت **گوشی** را به شکل قابل توجهی کاهش دهد.

3- بدون اینکه چیزی را تغییر داده باشید میزان مصرف دیتای شما به طور بی‌سابقه‌ای افزایش پیدا کند. فرآیندهای خراب‌کارانه می‌توانند در پیش‌زمینه و در حالیکه فعالیت‌های شما را رصد می‌کنند، حجم اینترنت شما را کاهش بدهند.

4- **گوشی** شما رفتار عجیبی دارد. اپ‌ها آنطوری که باید اجرا نمی‌شوند، به‌طور غیرمنتظره باز و بسته می‌شوند، یا اینکه اپ‌ها کرش می‌کنند یا اصلا نمی‌توانند باز شوند.

5- پاپ‌آپ‌ها روی صفحه **گوشی** ظاهر می‌شوند. اگر تعداد زیادی پاپ‌آپ روی صفحه ظاهر شد، به احتمال زیاد **گوشی** شما به **جاسوس‌افزار** یا **بدافزار** آلوده شده است.

از کجا بفهمیم چه کسی گوشی ما را هک کرده است

اول از همه سعی کنید تمام اپ‌هایی که برای شما ناشناخته است، شماره تلفن‌هایی که مشکوک هستند یا اکانت‌های مربوط به شبکه‌های اجتماعی که با آنها در تماس بوده‌اید را شناسایی کنید. یک جستجوی سریع می‌تواند تاحدودی

کارساز باشد، اما ردگیری **هکر**ها معولا نیاز به کارشناس **امنیت** سایبری دارد.

اما اگر گوشی هک شد چه کنیم

اگر گوشی شما هک شده است کارهای زیر را انجام دهید:

1- به‌سرعت تمام کلمات عبوری که استفاده می‌کنید را تغییر دهید.

2- خیلی سریع تمام نرم‌افزارهای مشکوک را پاک کنید.

3- به دوستان خود اطلاع دهید تا اگر پیام‌های مشکوک از طرف شما دریافت کردند گوش به‌زنگ باشند.

4- از انتشار هات‌اسپات شخصی خود در اماکن عمومی خودداری کنید چون این بهترین راه برای **هکر**هاست تا بتوانند وارد **گوشی** شما شوند.

5- حتما نرم‌افزار **امنیتی** موبایل نصب کنید. نرم‌افزار **امنیتی** موبایل دستگاه را برای پیدا کردن **بدافزار** جستجو می‌کند و ممکن است اپ‌های مهم و حساس را در برابر آسیب‌ها محافظت کنند.

6- با استفاده از تنظیمات کارخانه‌های **گوشی** خود را ریستور کنید. این روش برای زمانی مناسب است که تعداد زیادی پاپ‌آپ یا اپ‌های مخرب باعث شده‌اند تا کار کردن با **گوشی** برای شما سخت شده باشد.

چگونه گوشی خود را از هک شدن در امان نگه داریم

1- وقتی در اماکن عمومی هستید از انتشار هات‌اسپات شخصی خود خودداری کنید. اگر هم قصد انتشار آن‌را دارید حتما مطمئن شوید که تنظیمات موردنیاز را تا جایی که ممکن است امن کرده باشید.

2- از وای‌فای یا مکان‌های شارژ **گوشی** که به آنها اطمینان ندارید استفاده نکنید. ممکن است **هکر**ها با راه‌اندازی اکسس پوینت ساختگی اما با یک نام واقعی بتوانند داده‌های شما را به‌دست بیاورند یا حتی شما را ردیابی کنند. فراموش نکنید که اگر وای‌فای عمومی استفاده می‌کنید اما کار بیشتری برای انجام ندارید حتما آن را قطع کنید.

3- زمانی‌که از بلوتوث استفاده نمی‌کنید حتما آن را خاموش کنید چون **هکر**ها می‌توانند از آن به‌عنوان اکسس پوینت استفاده کنند.

4- **گوشی** خود را با تعریف کلمه عبور یا لاک اسکرین قفل کنید.

5- اجازه ندهید افرادی که آنها را نمی‌شناسید از **گوشی** شما استفاده کنند.

6- به‌طور مرتب اپ‌های روی **گوشی** را بررسی کنید تا متوجه اپ‌های ناشناخته بشوید.

7- پیام‌ها، لینک‌ها یا فایل‌های مشکوک را باز نکنید. شاید که **بدافزار** یا **جاسوس‌افزار** باشند.

8- اپ‌های ضد **بدافزار** نصب کنید و آنها را دائما به‌روزرسانی کنید.

9- از سایت‌های دانلودی که به آنها اطمینان ندارید استفاده نکنید. این سایت‌ها می‌توانند منبع احتمالی **بدافزار**ها باشند.

منبع:

تاریخ انتشار:
15 شهریور 1398

نشانی منبع:
https://www.shabakeh-mag.com/tricks/16002/%D8%A7%D8%B2-%DA%A9%D8%AC%D8%A7-%D8%A8%D9%81%D9%85%DB%8C%D9%85-%DA%A9%D9%87-%DA%AF%D9%88%D8%B4%DB%8C-%D9%85%D8%A7-%D9%87%DA%A9-%D8%B4%D8%AF%D9%87-%D8%A7%D8%B3%D8%AA%D8%9F