بسم الله الرحمن الرحیم

پلیس فتا، سایه سار امنیت در فضای مجازی

www.cyberpolice.ir

10 practical tips to enhance the security of Android

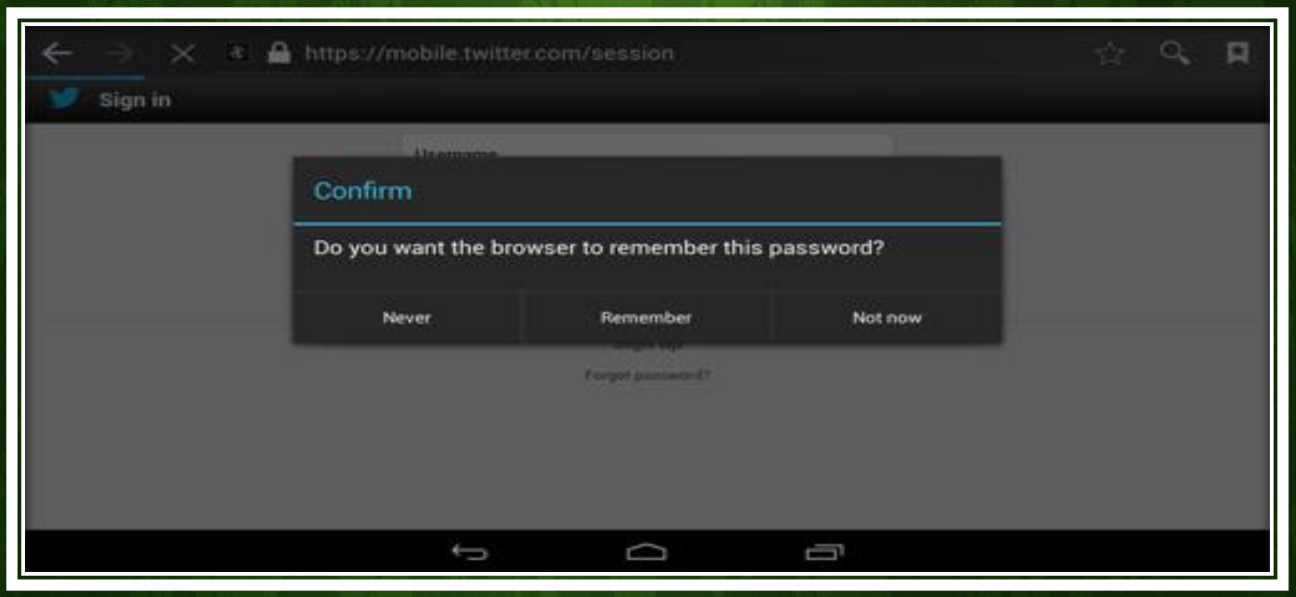
10 نکته
کاربردی برای ارتقاء امنیت تلفن های هوشمند

تلفن‌های هوشمند امروزی، علاوه بر قابل‌حمل بودن، اطلاعات شخصی ما را هم با خود حمل کنند! امروزه امنیت مسئله‌ای بزرگ است که شکسته‌شدن آن برای تلفن شما چیزی بیش ازدست دادن چند شماره تلفن خواهدبود! ما درباره حساب‌های شبکه‌های اجتماعی، فایل‌های شخصی و همگام‌سازی شده، اسناد مهم، ایمیل‌ها، تصاویر و پیام‌ها و چندین و چند مورد دیگر صحبت می‌کنیم! در این بین اندروید سیستم‌عاملی فراگیر و رایج است که کاربران بسیاری از آن استفاده می‌کنند، اساس اندروید هم منبع کاملاً باز یا به اصطلاح Open Sourceبودن است که به خودی خود می‌تواند امنیت گوشی شما را پایین بیاورد، پس با ما و ۱۰ نکته کاربردی جهت امنیت بیشتر دستگاه ، هوشمند همراه باشید.

۱

(از ذخیره کردن رمزهایتان بپرهیزید)

افراد زیادی هنگام ورود به حساب کاربری در شبکه‌ها و سایت‌های مختلف، password خود را save می‌کنند! که چندان نمی‌تواند کار درستی باشد، تا به حال به این فکر کردید که اگر فردی فقط برای چند ثانیه به دستگاه شما دسترسی داشته باشد می‌تواند به صورت کامل حساب شما را زیر و رو کند؟ پس بهتر است که در موارد مهم کمی بیشتر حواسمان به رمزهایمان باشد.)



۲

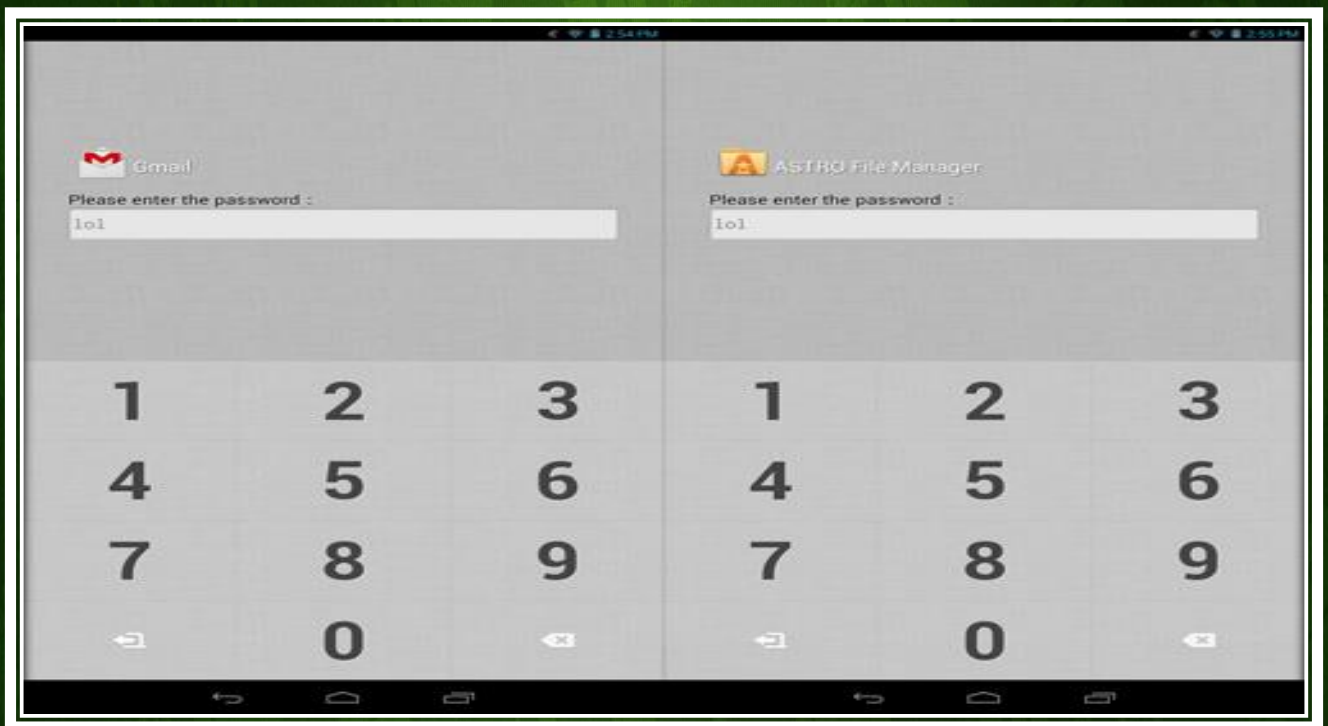
(استفاده از امکانات پیش‌فرض امنیتی اندروید)

اگر سری به تنظیمات دستگاه اندروید خود بزنید ، می‌بینید که بصورت پیش‌فرض نیز گزینه‌هایی برای شما تعبیه شده‌است .با تغییر قفل صفحه و انتخاب یکی از روش‌های Password, PIN, Pattern یا Face Unlock می‌توانید امنیت تجهیزات خود را تضمین کنید.

۳

(برای تمام برنامه های خود password بگذارید)

قفل کردن و رمزگذاری روی برنامه‌های مختلف، از آسان‌ترین و کاربردی‌ترین روش‌های امنیتی است نرم‌افزارهایی چون applock این کار را به راحتی برای شما، انجام خواهندداد! البته توجه کنید که تا حد امکان از رمزهایی مثل پترن استفاده نکنید چون از روی اثر به جا مانده روی نمایشگر، می‌توانند قابل تشخیص باشند!

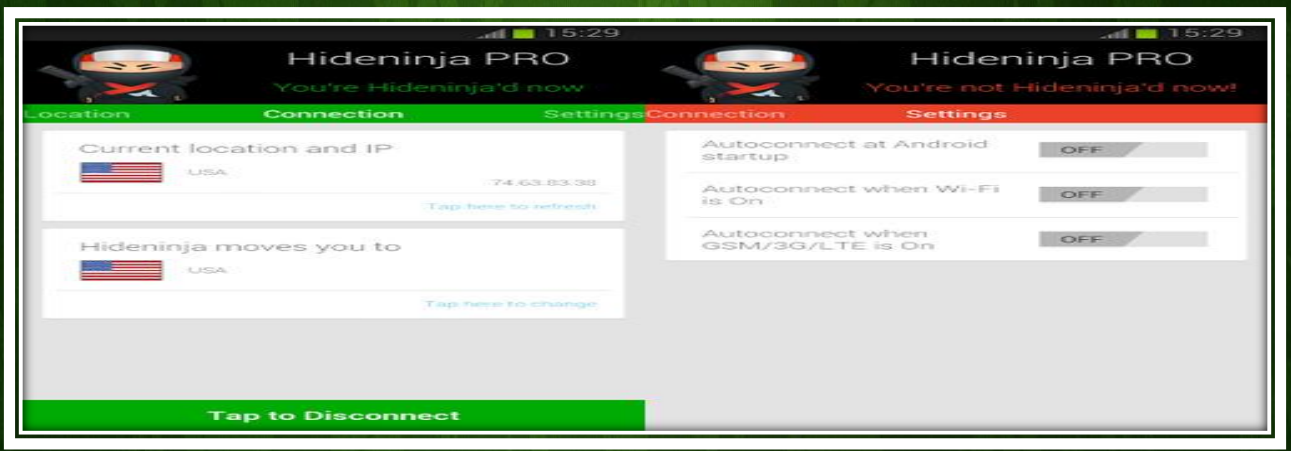


۴

(شبکه اینترنتی خود را ایمن سازی)

یکی از مهم‌ترین بخش‌های ایمن‌سازی یک دستگاه، امنیت شبکه‌ای است که به آن متصل می‌گردد. البته که بسیاری از افراد سودجو نیز، از همین راه به اطلاعات شما دسترسی پیدا می کنند! تا حد امکان سعی کنید از شبکه‌های wifi عمومی که در شهر وجود دارد، برای کارهای شخصی چون پرداخت‌های بانکی استفاده نکنید، چون از آن‌جایی که همه افراد از همان شبکه‌ای که شما استفاده می‌کنید، استفاده می‌کنند؛ و به راحتی می‌توانند اطلاعات شما را در زمانی بسیار کوتاه به سرقت ببرند.

شما می‌توانید با نرم‌افزارهای مختلف شبکه اتصالی خود را، کاملاً رمزگذاری و ایمن کنید، که برای افراد مختلف سرقت اطلاعات شما را بسیار سخت خواهدکرد



۵

(از حساب‌های کاربری مختلف استفاده نمایید)

اگر از یک تبلت اندرویدی استفاده می‌کنید، از نسخه جلی‌بین اندروید به بعد قادر هستید تا چند پروفایل مختلف در تبلت ایجاد کرده و برنامه‌ها و اطلاعات شخصی خود را از سایر افرادی که از تبلت استفاده می‌کنند، جدا سازید! برای استفاده از این امکان به مسیر Setting > " Users " بروید.

۶

(از اطلاعاتتان، یک نسخه پشتیبان بگیرید)

پشتیبان گیری از اطلاعات یک امر ضروری در دنیای تلفن‌های هوشمند امروزی محسوب می‌شود. وقتی را تصور کنید که دستگاه شما توسط شخصی به سرقت برده می‌شود، تنها راهی که شما می‌توانید از دسترسی به اطلاعاتتان جلوگیری کنید حذف تمامی آن‌ها از راه دور است. یعنی بدون داشتن یک نسخه پشتیبان جداگانه، برای همیشه تمامی اطلاعات را از دست خواهید داد.

۷

(از برنامه‌های امنیتی دیگر هم استفاده کنید)

با افزایش و قوی‌تر شدن روزبه‌روز بدافزارها، می‌توانید از آنتی‌ویرس‌ها و برنامه‌های امنیتی، جهت ایمن‌سازی سیستم عامل خود استفاده کنید .البته به این مورد نیز توجه کنید که هیچوقت به صورت همزمان دو یا چند آنتی‌ویروس روی دستگاه خود نصب نکنید، چرا که طبق گزارشات می‌تواند مشکلات سخت‌افزاری/نرم‌افزاری متعددی برای سیستم عامل ایجاد کند.

۸

(تلفن گم‌شده‌تان را ردیابی کنید)

نرم افزارهای مختلفی وجود دارند که مکان یابی گوشی را دنبال می کنند شما می توانید با نصب این نرم افزارها در زمان سرقت و یا مفقودی گوشی خود را در اسرع وقت پیدا نمایید

۹

(مراقب اپلیکیشن‌هایی که نصب می کنید، باشید)

گوگل اخیرا ۵۰۰۰۰ اپلیکیشن را که به عنوان نرم‌افزار مخرب شناسایی شده بودند، حذف کرده است .باید به این نکته توجه داشته باشید که تعداد اپلیکیشن‌هایی مانند نرم‌افزارهای مخرب، ویروس‌ها یا سایر نرم‌افزارهایی که به صورت مخفیانه اطلاعات شما را به سرقت می‌برند و به گوشی شما آسیب می‌رسانند، کم نیست .در بررسی‌های صورت گرفته، مشخص شده که ۹۵ درصد از نرم‌افزارهای مخرب با هدف آلوده کردن دستگاه‌های اندرویدی تولید می‌شوند و همین بدافزارها توانسته‌اند تعداد قابل توجهی دستگاه اندرویدی را آلوده کنند.

۱۰

(وایرلس و بلوتوث را خاموش کنید)

وقتی که در خانه نیستید، بهتر است که وایرلس و بلوتوث خود را خاموش کنید. هر زمان که به یک شبکه‌ی بی‌سیم نامطمئن متصل شوید، به هکرها اجازه داده‌اید تا از طریق شبکه، اطلاعات شما را به صورت اجمالی بررسی کنند. حتی اگر در حال انجام عملیات بانکی یا کارهای دیگری که به اطلاعات حساس نیاز دارند، نباشید، با این حال هکر می‌تواند با اتصال به گوشی هوشمند شما، اطلاعات و... را به سرقت ببرد.

وقتی راجع به بلوتوث صحبت می‌کنیم، می‌بینیم که هک شدن از این طریق کمتر رواج دارد. اما زمانی به محبوبیت آن اضافه می‌شود که مردم از تکنولوژی‌هایی فراتر از هدست استفاده می‌کنند. امروزه شما ساعت‌هایی دارید که با تلفن‌تان از طریق بلوتوث در ارتباط است. اگر بلوتوث روشن و قابل مشاهده باشد، راهی برای هکرها ایجاد می‌کند تا بتوانند داده‌هایی را که بین دستگاه بلوتوثی و تلفن شما رد و بدل می‌شوند را ببینند.