

آیا "ریست فکتوری" موبایل باعث حذف اطلاعات می‌شود!



ریست فکتوری به معنای برگرداندن تنظیمات گوشی به حالت اولیه یعنی تنظیمات کارخانه است. اما باید بدانید با این عمل اطلاعات گوشی پاک نمی‌شود. برای آشنایی بیشتر با این موضوع با ما همراه باشید.

برخی افرادی که قصد فروختن گوشی خود را دارند آن را به حالت ریست فکتوری در می‌آورند و فکر می‌کنند اطلاعات گوشی شان پاک می‌شود اما باید بدانید نرم افزار هایی وجود دارد که امکان بازیابی اطلاعات گوشی را به شما می‌دهد حتی بعد از ریست فکتوری. برای جلوگیری از دسترسی به اطلاعات گوشی باید آنها را رمزگذاری کنید. با پرشین وی همراه باشید تا با چگونگی انجام این کار آشنا شوید.

تاثیر ریست فکتوری گوشی بر اطلاعات آن

با پیشرفت تکنولوژی و آمدن نسل جدید تلفن های همراه، دیگر کمتر کسی پیدا می شود که از نسل قدیمی این تلفن ها استفاده کند و همه به نوعی جذب امکانات گوشی های هوشمند شده اند.

بسیاری از افراد پس از مدت زمانی که از گوشی های هوشمند استفاده می کنند، به هر دلیلی اقدام به فروش آن ها می کنند و هرکسی در هنگام فروش یا دادن دستگاه تلفن همراه به شخصی دیگر برای اینکه خیالش را راحت کند اولین اقدامی که انجام میدهد، حذف اطلاعات گوشی همراه خود است و برای این کار از ریست فکتوری (بازگشت به تنظیمات کارخانه) استفاده می کنند و تصور می کنند با انجام این کار اطلاعات گوشی های شان حذف می شود و دیگر قابل بازیابی نیست. اما این تصور اشتباه است.

بسیاری از تحقیقات صورت گرفته نشان می دهد، اطلاعات گوشی ها حتی پس از آن که کاربران آن ها را به تنظیمات کارخانه (ریست فکتوری) برمی گردانند، باز هم اطلاعات قابل دستیابی و بازگشت است و کسانی که تلفن های همراه شما را خریداری می کنند می توانند با استفاده از نرم افزار هایی، اطلاعات شما را بازگردانند و به آن ها دسترسی پیدا کنند.



ریست فکتوری موبایل

دلیل این است که حتی پس از این کار اطلاعات قبلا ذخیره شده توسط اطلاعات جدید overwritten یا بازنویشته نمی‌شوند. درست همانند دیسک‌های سخت کامپیوتر یا هاردهای قابل حمل در اینجا نیز اطلاعات پس از حذف و تا زمان ذخیره شدن فایل بعدی باقی می‌مانند و متأسفانه برخی ابزارهای بازیابی فایل وجود دارند که می‌توانند این نوع فایل‌های مخفی شده روی دیسک سخت را بازیابی کنند.

درواقع یکی از خطراتی که همیشه کاربران را تهدید می‌کند، بازیابی اطلاعاتی است که به خیال آن‌ها حذف شده است و یکی از بزرگ‌ترین مشکلات به خطر افتادن حریم شخصی افراد می‌باشد و برای جلوگیری از چنین رخدادی راه حلی وجود دارد.

رمزگذاری تلفن همراه و سپس بازگشت به تنظیمات کارخانه

رمزگذاری، مطمئن‌ترین راه برای جلوگیری از بازیابی اطلاعاتی است که فکر می‌کنید حذف شده اند. با این روش شما اطلاعات خود را قفل می‌کنید و فقط با وارد کردن کلماتی که شما آن‌ها را انتخاب کرده اید، اطلاعات قابل دسترسی هستند و دیگر تلفن همراه شما بدون وارد کردن گذرواژه قابل دسترسی نخواهد بود.

چگونه بر روی تلفن همراه خود رمز گذاری کنیم؟

گوشی‌هایی که سیستم عامل آن‌ها مجهز به اندروید ۶ هستند، نیازی به این تنظیمات ندارند و توسط شرکت گوگل به طور اجبار رمز گذاری می‌شوند و بیشترین ضریب امنیتی را دارند و دسترسی به آن‌ها کار آسانی نیست.

اما اگر سیستم عامل شما مجهز به اندروید ۵ به پایین است، می‌توانید با استفاده از شیوه زیر، از امکان رمزگذاری روی اطلاعات در گوشی خود استفاده کنید.

نکته قابل ذکر این است که فقط برخی از تلفن‌های همراه از چنین قابلیت بهره می‌برند و این ترفند

فقط مخصوص گوشی های اندروید است و دلیل آن این است که حتی پس از این کار اطلاعات قبلا ذخیره شده توسط اطلاعات جدید overwritten یا بازنویسه نمی شوند. درست همانند دیسک های سخت کامپیوتر یا هاردهای قابل حمل در اینجا نیز اطلاعات پس از حذف و تا زمان ذخیره شدن فایل بعدی باقی میمانند و متاسفانه برخی ابزارهای بازیابی فایل وجود دارند که میتوانند این نوع فایل های مخفی شده روی دیسک سخت را بازیابی کنند.



نحوه ریست فکتوری موبایل

برای این کار کافیست وارد Settings تلفن همراه خود شوید، سپس وارد بخش Security شوید و با ورود به بخش Encrypt phone یا Encrypt Device رمز عبور را به دلخواه خود انتخاب کنید.

Settings > Security > Encrypt phone

توصیه میکنیم اگر قصد فروش گوشی خود را دارید ابتدا گوشی را از این طریق رمزگذاری کرده و بعد "factory reset" (بازگشت به تنظیمات کارخانه) را انجام دهید. با این کار اطلاعات گوشی به سختی قابل بازیابی خواهد بود.

اکنون که رمزگذاری گوشی و "factory reset" را انجام داده اید میتوانید مطمئن باشید که اطلاعات شما از روی گوشی پاک شده است اما اگر مایل باشید از این هم فراتر بروید میتوانید بعد از انجام مراحل بالا با ذخیره

کردن اطلاعات بی فایده روی گوشی از نابودن شدن اطلاعات ذخیره شده روی گوشی‌تان اطمینان بیشتری حاصل کنید.

برای اینکار بعد از "factory reset" گوشی را دوباره آماده استفاده کنید و بدون اینکه وارد اکانت گوگل خود شوید و پس از راه‌اندازی گوشی دکمه ذخیره ویدیو را با کیفیت و رزولوشن بالا فشار دهید و تا زمانی که فضای گوشی پر نشده به فیلمبرداری ادامه دهید. حالا دوباره "factory reset" کنید.

با تکرار این کار می‌توانید به طور کامل از پاک شدن اطلاعاتتان مطمئن شوید.

بیشتر بدانید ریست فکتوری از تنظیمات دستگاه

۱- ابتدا به تنظیمات دستگاه اندرویدی خود بروید.

۲- در لیست تنظیمات بخش Backup & reset را پیدا کرده و وارد آن شوید.

۳- حال برای ریست فکتوری اندروید، Factory Data Reset را لمس کنید.

۴- در این صفحه دستگاه اندرویدی به شما هشدار می‌دهد که با انجام این کار تمام اطلاعات شما، حساب‌های کاربری، برنامه‌ها، و... از دستگاه حذف خواهند شد. با لمس Reset یا Delete All از انتهای صفحه تصمیم خود را تایید کنید تا پروسه ریست فکتوری آغاز شود.

در صورتی که موبایل یا تبلت اندروید شما رمز داشته باشد، در این مرحله از شما پرسیده خواهد شد تا از ریست شدن دستگاه به دست دیگران جلوگیری شود.

منبع: persianv.com

ظرفیت گروه‌های تلگرام ۷۵ هزار نفری شد!



هر روز به قابلیت های تلگرام افزوده می شود و به نظر نمی رسد پاول دورف به این زودی ها دست از افزایش ویژگی‌های این پیام رسان بکشد.

به گزارش جام جم آنلاین به نقل از دیجی رو، شاید این تعداد کاربر برای یک گروه پیام رسان بسیار زیاد باشد و کمتر کسی بتواند از پس کنترل چنین گروهی بر آید. اما با این حال هستند گروه هایی که هم اکنون به مرز ۵۰ هزار کاربر رسیده اند و افزایش ظرفیت گروه‌ها تا مدتی می تواند محدودیت عضوگیری آنها را از بین ببرد.



منبع: جام جم آنلاین

پردا نلودترین اپلیکیشن جهان
معرفی شد.



اپلیکیشن پیام‌رسان واتس‌آپ، سال ۲۰۱۷ میلادی بیشترین تعداد دانلود را در فروشگاه‌های اینترنتی داشته است.



به گزارش جام جم آنلاین به نقل از ایسنا، اپلیکیشن واتس‌آپ که به گفته کارشناسان، همواره از امن‌ترین، محبوب‌ترین و پرمردارترین پیام‌رسان‌های جهان شناخته شده است، حالا طبق گزارش جدیدی از سوی موسسه تحقیقاتی اپ توپیا، تعداد دفعات دانلودهای این پیام‌رسان در سال ۲۰۱۷ میلادی از مرز یک

میلیارد هم گذشت و آن را به پردانلودترین اپلیکیشن در فروشگاه‌های اینترنتی و آنلاین جهان تبدیل کرد.

بر اساس گزارش‌های رسمی منتشر شده توسط واتس‌آپ، این اپلیکیشن حدود ۳/۱ میلیارد کاربر در سراسر جهان دارد. شرکت فیسبوک با در اختیار داشتن واتس‌آپ در سال ۲۰۱۴، حدود ۱۹ میلیارد دلار درآمد کسب کرد و هم اکنون نیز درصدد جلب رضایت کاربران و افزایش تعداد دفعات دانلودها از این اپلیکیشن پیام‌رسان محبوب است. فیسبوک مسنجر نیز یکی دیگر از پیام‌رسان‌های اختصاصی فیسبوک است که همراه واتس‌آپ از پرطرفدارترین پیام‌رسان‌های جهان هستند.

فهرست موسسه تحقیقاتی اپ توپیا که به ترتیب شامل تعداد دفعات دانلود و نصب اپلیکیشن‌های مذکور توسط کاربران در سال ۲۰۱۷ میلادی است، شامل هشت اپلیکیشن برتر و پرطرفدار می‌شود. ادم بلاکر، مدیر ارتباطات موسسه اپ توپیا در این باره خاطرنشان کرده است ممکن است یک کاربر روی چند دستگاه الکترونیکی متصل به اینترنت خود، این اپلیکیشن را دانلود و استفاده کند، بنابراین نباید این‌طور تصور شود که تعداد دانلودها با تعداد کاربرانی برابر است که از این اپلیکیشن استفاده می‌کنند.

از دیگر اپلیکیشن‌هایی که پس از واتس‌آپ در این فهرست جای گرفته‌اند، می‌توان به ترتیب به Subway Surfers (بخش بازی)، Netflix (بخش تفریح و سرگرمی)، Subway (بخش خوراکی)، Tinder (بخش ارتباطات)، Uber (بخش حمل و نقل)، AliExpress (بخش خرید و فروش) و Spotify (بخش موسیقی) اشاره کرد.

منبع: جام جم آنلاین

چگونه آخرین بازدید در اینستاگرام را غیرفعال کنیم؟



اگر نمی‌خواهید قابلیت آخرین بازدید در اینستاگرام که به تازگی به این اپلیکیشن اضافه شده فعال باشد، ما در این مقاله به شما آموزش می‌دهیم تا به راحتی آن را با استفاده از گزینه Show Activity Status غیرفعال کنید.

به گزارش جام‌جم آنلاین به نقل از گجت‌نیوز، شبکه‌های اجتماعی همیشه راه‌های جدیدی را برای به خطر انداختن حریم خصوصی شما به وجود می‌آورند و در سال ۲۰۱۸، نخستین تنظیم آزاردهنده جدید را این بار در اینستاگرام شاهد هستیم. این اپلیکیشن به دنبال به‌روزرسانی جدیدی که دریافت کرد، حالا صاحب یک قابلیت جدید شده است که به افراد دنبال کننده به علاوه هر کسی به شما پیامی را ارسال کرده، آخرین بازدید در اینستاگرام توسط شما را مشاهده کنند.

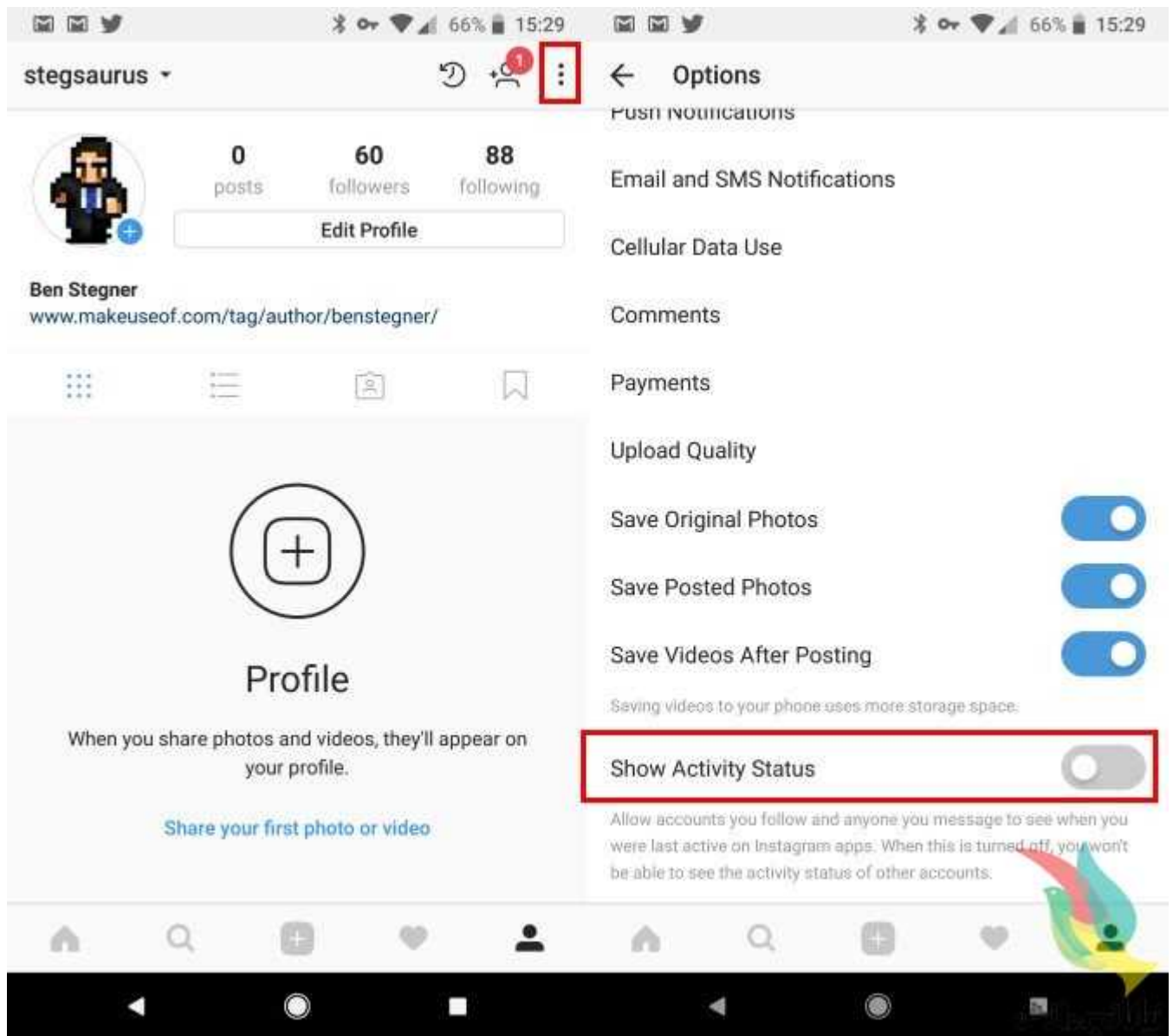
اگرچه این یک ویژگی خیلی مخرب نیست، اما به سایر افراد اجازه می‌دهد تا ببینند هر ثانیه از روز شما مشغول چه کاری هستید، این درحالیست که شاید نخواهید هر زمان مشغول اینستاگرام گردی بودید کاربران دیگر از آن مطلع باشند. و از آنجایی که اینستاگرام بدون آن که کسی مطلع باشد، به محض آپدیت این اپلیکیشن قابلیت نمایش آخرین بازدید در اینستاگرام را فعال می‌کند، بسیاری از کاربران نمی‌دانند که از کجا باید اقدام به غیرفعال کردن این ویژگی کنند. ما در این مطلب به شما آموزش خواهیم داد. کافیت مراحل زیر را دنبال کنید.

آموزش غیرفعال کردن آخرین بازدید در اینستاگرام

اینستاگرام را بر روی گوشی آیفون یا دیوایس اندرویدی خود اجرا کنید. با ضربه بر روی نماد شبه مانند سمت راست قسمت پایین نوار ابزار، به صفحه پروفایل اینستاگرام خود بروید.

کاربران آی او اس بر روی آیکن چرخ دنده Settings رفته و سپس دکمه‌ی Edit Profile را بزنند. کاربران اندروید باید در سمت راست، قسمت بالای صفحه بر روی دکمه ۳ نقطه ضربه بزنند.

به قسمت پایین منو تنظیمات بروید، یک گزینه جدید به نام Show Activity Status را مشاهده خواهید کرد. کافیت آن را به حالت غیرفعال درآورید تا قابلیت آخرین بازدید در اینستاگرام شما به طور کلی غیرفعال شود.



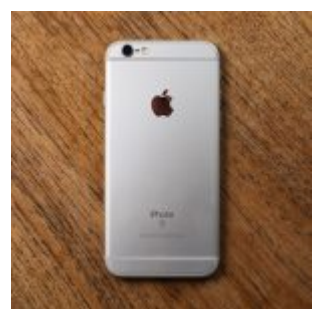
زمانی که این گزینه را به حالت غیرفعال درمی‌آورید، علاوه بر این که کاربران دیگر نمی‌توانند آخرین زمان حضور شما در این اپلیکیشن را مشاهده کنند، شما نیز دیگر قادر نخواهید بود متعاقباً آخرین بازدید دنبال کنندگانتان را در اینستاگرام مشاهده کنید. اگر این قابلیت به صورت فعال باقی بماند، می‌توانید آخرین بازدید تمامی دوستانتان را در لیست پیام‌های دایرکت مشاهده کنید؛ البته اگر آنها هم این قابلیت را غیرفعال نکرده باشند.

حالا آزادانه اینستاگرام گردی کنید.



منبع: جام جم آنلاین

کشف حفره امنیتی که آیفون را فریز می‌کند



آبراهام ماسری، توسعه دهنده نرم‌افزاری، باگس به نام ChaiOS پیدا کرده که از آن طریق آیفون فریز می‌کند.

به گزارش خبرآنلاین، این برنامه‌نویس که کد مخصوص را روی سایت گیت‌هاب گذاشته می‌گوید با ارسال لینک روی آی مسیج می‌توان باعث کرش کردن گوشی آیفون اپل شد.



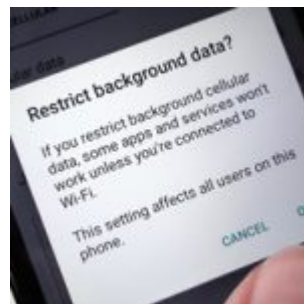
وی در حال قراردادن کدهای تصادفی روی آیفون بود که این باگ را کشف کرد.

آبراهام میگوید این کد مخرب روی آیفون ۵ اس و ایکس و آی او اس ۱۰ تا ۱۱٫۲٫۵ تست شده و آنها را درگیر کرده است.

سخنگوی اپل ضمن تایید این مشکل، گفت وصله امنیتی چند روز آینده به صورت آپدیت نرم‌افزاری به گوشی‌های آیفون خواهد رسید.

منبع: بیتوته

اعمال محدودیت دسترسی برنامه‌های اندرویدی به اینترنت

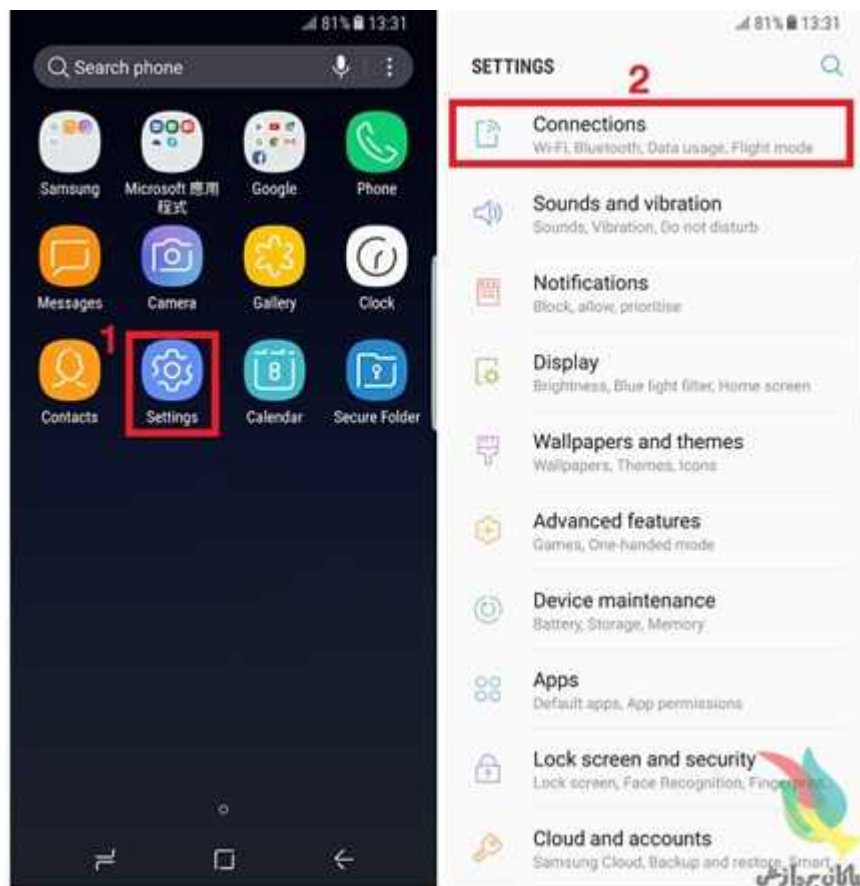


تاکنون چند مرتبه این اتفاق ناخوشایند را تجربه کرده‌اید که برنامه‌های کاربردی گوشی اندرویدی شما بدون اطلاع به اینترنت متصل شده‌اند، داده‌هایی را دریافت کرده یا ارسال کرده‌اند؟ ما در این مقاله راهکار جالبی را به شما معرفی می‌کنیم تا ضمن صرفه‌جویی در پهنای باند بتوانید مانع از آن شوید تا برنامه‌ها در پس‌زمینه و به دور از چشم شما به اینترنت متصل شوند.

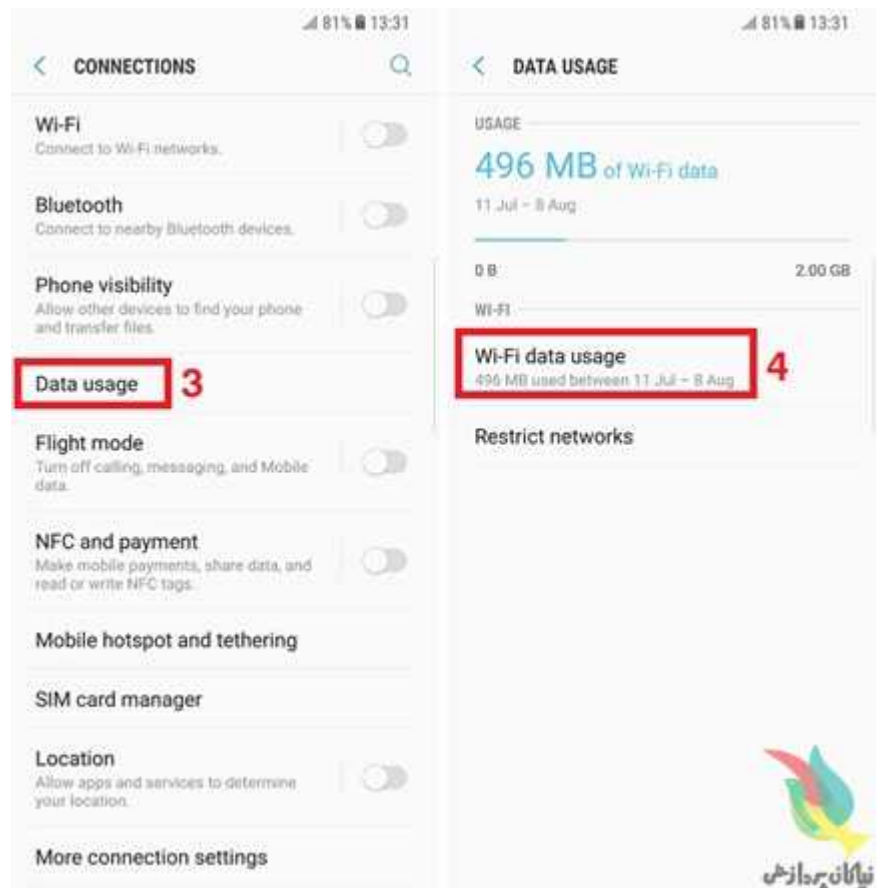
کاربران اندرویدی یک راهکار ساده اما ایده‌آل در اختیار دارند که به آن‌ها اجازه می‌دهد دسترسی برنامه‌های خاص به اینترنت را مسدود کنند. با توجه به این‌که امروزه برنامه‌های زیادی روی دستگاه اندرویدی شما نصب می‌شوند، جای تعجب نیست که بسیاری از این برنامه‌ها بدون اطلاع شما به اینترنت متصل شوند. این اتفاق از آن جهت ناخوشایند است که به شکل قابل توجهی سرعت اینترنت شما را کند کرده و مهم‌تر از باعث می‌شوند اینترنت شما به سرعت مصرف شود. اما برای حل این مشکل شما می‌توانید از قابلیت پیش‌فرض اندروید یا برنامه‌هایی که در ادامه با آن‌ها آشنا خواهید شد استفاده کنید.

راهکار شماره اول، از طریق تنظیمات گوشی

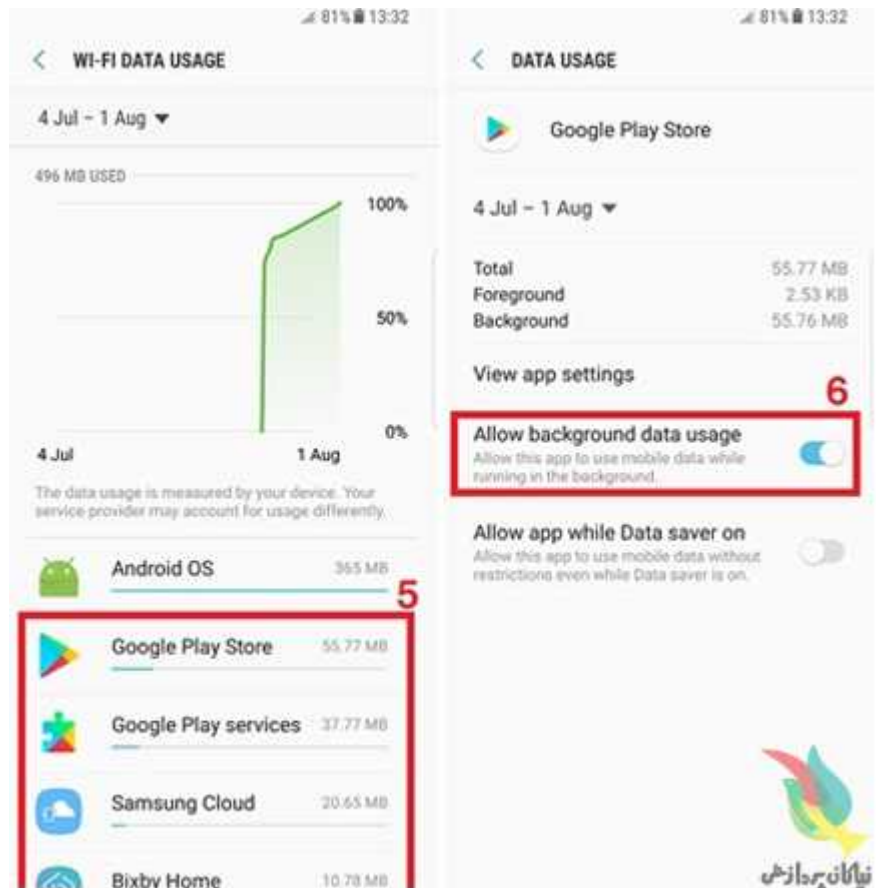
گام اول، در گوشی اندرویدی (سامسونگ) به بخش Settings بروید. اکنون گزینه Connections را انتخاب کنید.



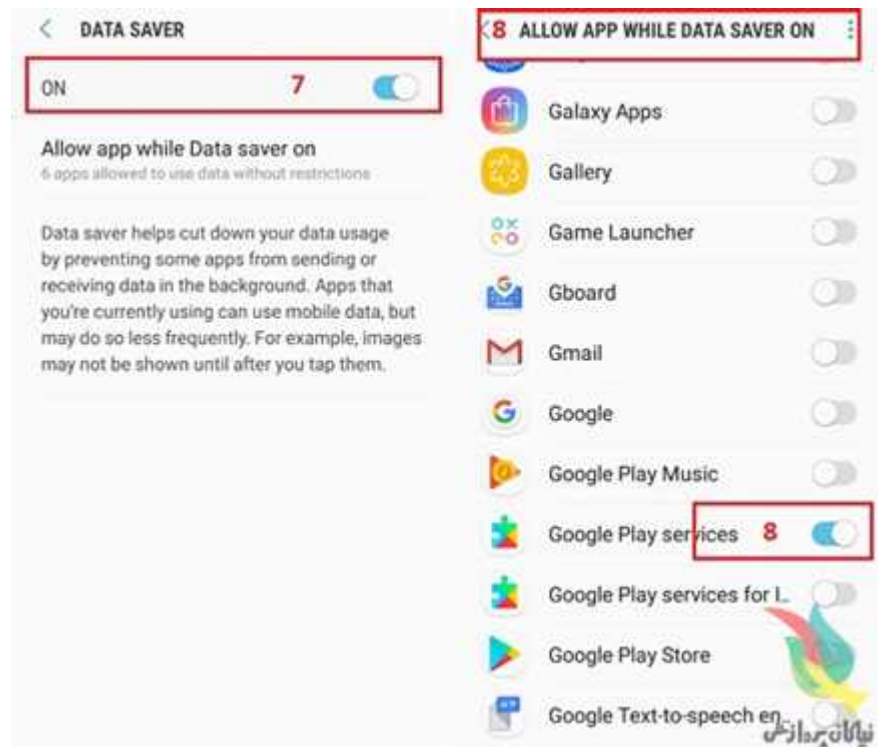
گام دوم، اکنون گزینه Data usage را انتخاب کرده و در ادامه گزینه Wi-Fi را انتخاب کنید.



گام سوم، یک برنامه کاربردی را انتخاب کنید. با انتخاب برنامه به صفحه‌ای وارد می‌شوید که در آن گزینه‌ای به نام اجازه مصرف داده‌ها در پس‌زمینه وجود دارد. اگر گزینه Allow background data usage فعال باشد، یک برنامه کاربردی می‌تواند در پس‌زمینه دستگاه به اینترنت متصل شده و داده‌هایی را از آن دریافت کند.



همین تکنیک را در ارتباط با زمانی که از اینترنت موبایلی استفاده می‌کنید نیز می‌توانید به کار ببرید. همچنین فراموش نکنید که گزینه Data Saver را روی گوشی خود فعال کنید. پس از فعال‌سازی این قابلیت گزینه Allow app while Data save On را لمس کنید. صفحه‌ای ظاهر می‌شود که از طریق آن می‌توانید برنامه‌هایی که این گزینه در ارتباط با آن‌ها به کار گرفته خواهد شد را فعال کنید. فعال بودن این گزینه به میزان قابل توجهی در مصرف اینترنت صرفه‌جویی می‌کند.



راهکار دوم، به کارگیری برنامه‌های ثالث

اگر ترجیح می‌دهید به شکل سفارشی‌تری اینکار را انجام دهید، برنامه‌های ویژه‌ای برای این منظور وجود دارند.

Mobiwol: بدون نیاز به روت کردن دستگاه

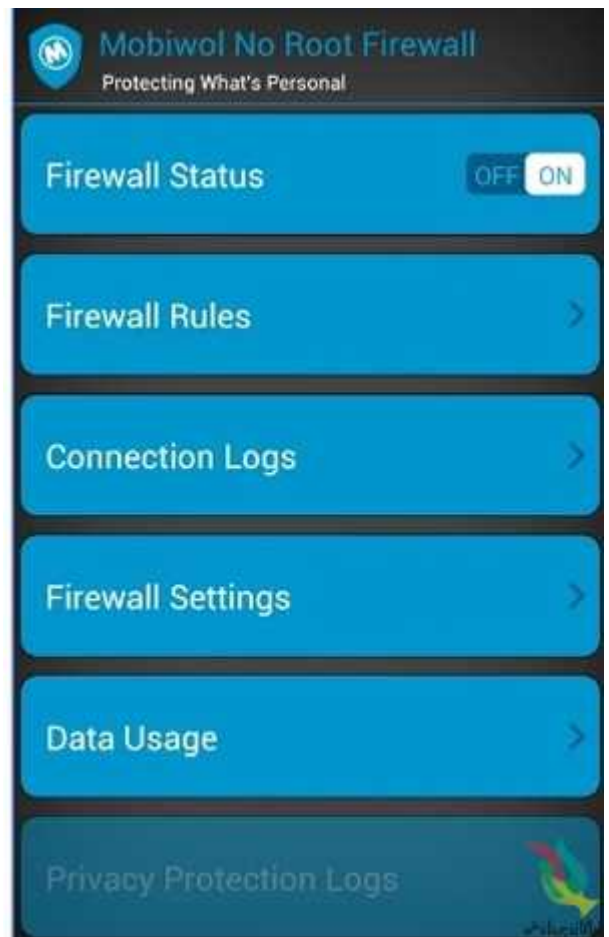
گام اول، ابتدا برنامه Mobiwol را از فروشگاه گوگل پلی دانلود کرده و روی گوشی خود نصب کنید

گام دوم، برنامه را اجرا کنید. با این‌کار گزینه به نام Firewall Rules مشاهده می‌کنید. آنرا لمس کنید.

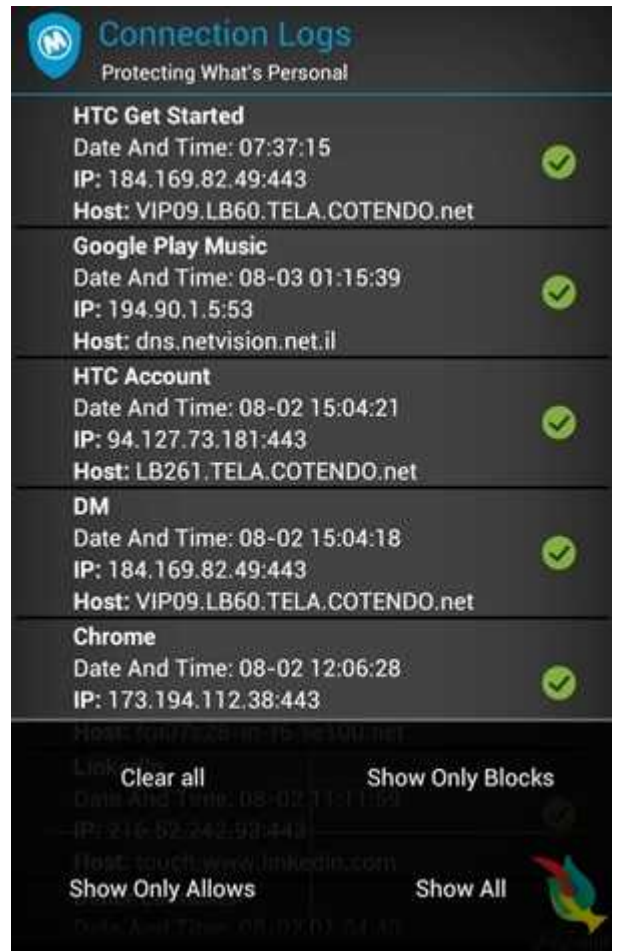
گام سوم، اکنون فهرستی از برنامه‌های کاربردی که روی گوشی شما نصب شده‌اند را مشاهده می‌کنید. در مقابل هر کدام از این برنامه‌ها دو گزینه وجود دارد. یکی از این گزینه‌ها اجازه دسترسی به وای‌فای و دیگری اجازه دسترسی به اینترنت موبایلی در پس‌زمینه دستگاه را به برنامه کاربردی تخصیص می‌دهند.



گام چهارم، پس از تنظیم گزینه‌های موردنظر به صفحه قبلی بازگشته و گزینه Firewall را روشن کنید. در پیغام ظاهر شده دکمه ok را لمس کنید.

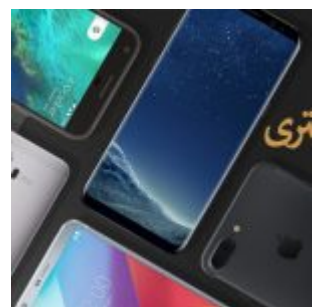


تمام شد، اکنون شما دسترسی به اینترنت برای برنامه‌هایی که مشخص کرده‌اید را با محدودیت روبرو کرده‌اید.



در این حالت برنامه Mobiwol گزارشی در این ارتباط به شما نشان می‌دهد.

آموزش رجیستری گوشی



همان طور که مطلع هستید مدتی است که طرح رجیستری گوشی و تبلت به مرحله اجرا رسیده و بدین ترتیب با خرید گوشی و تبلت جدیدی که مشمول این طرح شود، باید مراحل را برای ثبت آن در شبکه مخابراتی ایران طی کنید. در این مطلب، آموزش رجیستری گوشی در شبکه مخابراتی را با دو روش مختلف برای‌تان

قرار داده ایم.

آموزش رجیستری گوشی می‌تواند بسیاری از افراد را از سردرگمی رها کند؛ بنابراین برای رجیستر کردن دستگاه خریداری شده خود با ما همراه باشید.

رجیستری گوشی در شبکه مخابراتی به چه معناست؟

بر اساس قوانینی که به تازگی توسط وزارت ارتباطات و فناوری اطلاعات و سازمان تنظیم مقررات و ارتباطات رادیویی به اجرا در آمده، افرادی که گوشی جدیدی خریداری می‌کنند، باید آن را در شبکه مخابراتی به ثبت برسانند تا گوشی خریداری شده بتواند با توجه به نوع سیمکارت به شبکه مخابراتی ایران متصل شود. در واقع رجیستر کردن گوشی، به عنوان یک مجوز برای دستگاه تلقی می‌شود که آیا این مدل می‌تواند به شبکه مخابراتی اتصال داشته باشد یا نه.

فاز دوم این طرح که از تاریخ ۱۴ آذر امسال به اجرا رسید، در ابتدا تنها تبلت‌ها و گوشی‌های اپل را شامل می‌شد اما بر اساس اخبار جدید (هرآنچه درباره رجیستری گوشی باید بدانیم)، محصولات تولید کنندگان بیشتری نیز در آینده مشمول این طرح می‌شوند.

اگر دستگاه را رجیستر نکنم، چه می‌شود؟

در صورتی که گوشی یا تبلت مشمول‌تان در زمان طرح رجیستری خریداری شده باشد و نسبت به ثبت آن اقدام نکرده باشید، بعد از گذشت ۳۰ روز استفاده، سیمکارت موجود در دستگاه دیگر شناخته نشده و نمی‌تواند به شبکه مخابراتی ایران متصل شود. این قضیه برای گوشی مسافران هم صادق بوده و این دسته از افراد تنها ۳۰ روز می‌توانند بدون رسیدگی به شرایط و ضوابط گمرک از دستگاه‌شان استفاده کنند.

چگونه گوشی و یا تبلت را رجیستر کنم؟

دو راه برای رجیستر کردن دستگاه الکترونیکی شما وجود دارد. یکی با استفاده از وبسایت و دیگری توسط کد USSD بوده که در ادامه هر دو را برایتان توضیح داده ایم:

آموزش رجیستری گوشی با استفاده از وبسایت

وارد سایت سامانه هوشمند مدیریت تجهیزات ارتباطی (همتا) شوید.

شماره تلفن همراه خود را وارد کرده و بر روی ادامه بزنید.

ورود

انتخاب شماره تلفن همراه با شماره ملی

شماره ملی ☐ شماره تلفن همراه ☒

شماره تلفن همراه خود را وارد نمایید

ادامه

ثبت نام

برای استفاده بیشتر از امکانات سامانه ثبت نام کنید

ثبت نام

فراموشی رمز عبور

جهت استفاده از کد ملی از «استفاده نمایید»

بازیابی

فعال سازی

استعلام اصالت

نیان پردازش

کد ارسال شده توسط پیامک را به همراه کد تصویر امنیتی وارد کرده و بر روی ورود کلیک کنید.

ورود با شماره همراه

رمز عبور موقت ارسال شده به شماره 09979827936 را وارد کنید

رمز عبور ارسال شده را وارد نمایید

پنج هزار و چهارصد و یک

کد امنیتی را به عدد وارد نمایید

ورود

ارسال مجدد رمز عبور موقت
01:55

فراموشی رمز عبور

بازیابی

فعال سازی

استعلام اصالت

نیانان پردازش

با وارد شدن به صفحه جدید، از نوار سمت راست، بر روی فعال سازی تلفن همراه کلیک کنید.



شماره تلفن همراه، شناسه IMEI دستگاه و کد فعالسازی را وارد نمایید.

در آخر بر روی فعالسازی کلیک کرده و تغییرات را اعمال کنید.

آموزش رجیستری گوشی با استفاده از سامانه USSD

شماره *۷۷۷۷# را توسط دستگاه شماره گیری کنید.

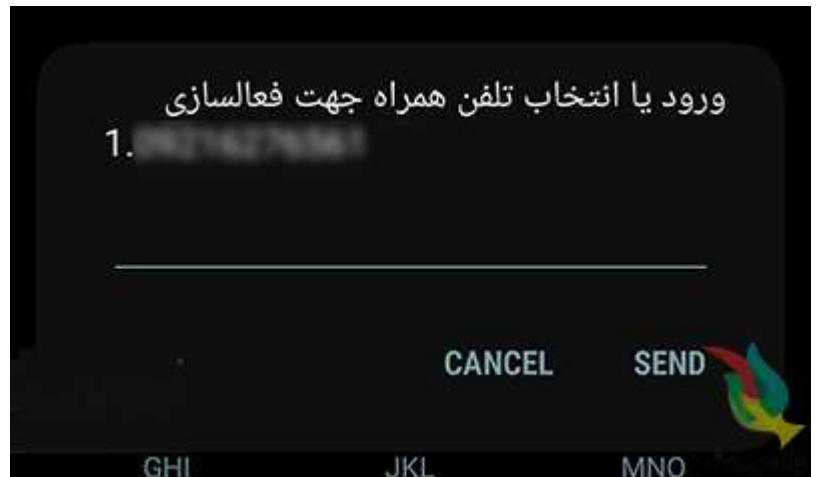
بعد از باز شدن سامانه، با شماره گیری ۲ و دکمه Send، گزینه فعالسازی را انتخاب کنید.



شناسه IMEI دستگاه را وارد نمایید.



شماره تلفن همراه خود را وارد کنید.



کد فعال سازی را وارد نمایید.



ثبت دستگاه را با ارسال عدد ۱ تایید کنید و منتظر پیامک اتمام مراحل بمانید.

برای رجیستری گوشی و تبلت توسط وبسایت و USSD، به موارد زیر توجه کنید:
در صورت موفق بودن عملیات ثبت دستگاه، پیامک تایید برای تان ارسال می‌گردد.
کد فعالسازی هنگامی که گوشی را خریداری می‌کنید، توسط فروشنده در اختیار تان قرار می‌گیرد.

شناسه IMEI دستگاه از روی جعبه و یا معمولاً در مسیر Settings -> About -> Status -> IMEI information phone -> گوشی قابل دسترسی است.

توسط اپلیکیشن سامانه هم‌تا که برای اندروید و iOS موجود بوده هم می‌توانید دستگاه خود را ثبت و کنترل کنید.



خرید و فروش گوشی و تبلت دست دوم به چه صورت انجام میشود؟

در صورتی که دستگاهی که می خواهید بخرید و یا بفروشید مشمول طرح رجیستری باشد، باید شماره ثبت شده را توسط وبسایت یا سامانه #۷۷۷۷* و بخش انتقال مالکیت، تغییر دهید.

منبع: بیتوته

دسترسی به عکسهای پاک شده در تلفن همراه



برخلاف تصور شما عکسهای پاک شده در تلفن همراهتان به راحتی قابل دسترسی اند!

دسترسی دوباره به عکسهایی که از تلفن هوشمندتان پاک می کنید، بسیار آسان بوده و همین موضوع می تواند گاهی اوقات بسیار مشکل ساز باشد.

برای مثال حالتی را در نظر بگیرید که می خواهید گوشی خود را که صدها عکس شخصی در آن ذخیره کرده اید، بفروشید. در این وضعیت خیلی راحت وارد گالری می شوید و با انتخاب گزینه Delete All همه عکسها

را پاک می‌کنید و یا کل گوشی را ریست فکتوری می‌کنید.

در این حالت با این فکر که عکسهایتان برای همیشه پاک شده، گوشی را تحویل شخص خریدار می‌دهید. اما چیزی که خبر ندارید این است که شخص خریدار به راحتی می‌تواند با این روش، به تمامی عکسهای ذخیره شده شما در حافظه داخلی، دسترسی پیدا کند.

اما برای جلوگیری از این موضوع چه کاری باید انجام داد؟

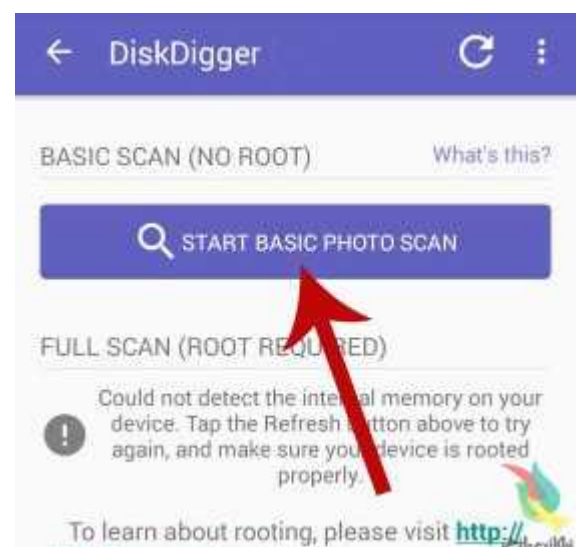
در واقع شما باید با انجام عملیاتی، عکسها را به‌صورتی پاک کنید که در آینده با هیچ روشی قابل بازگردانی نباشند.

برای انجام این کار در گوشی‌های اندرویدی مراحل زیر را به ترتیب طی کنید:

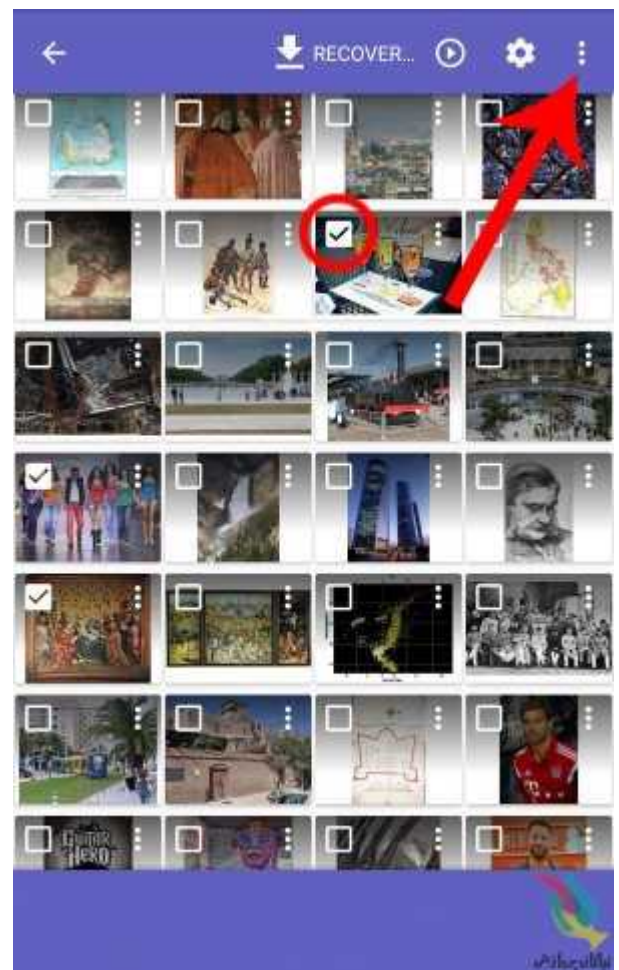
عکس‌هایتان را به همان روش معمولی با انتخاب گزینه Delete در گالری، حذف نمایید.

اپ DiskDigger را از اپاستور دانلود و نصب کنید. این برنامه در دو نسخه رایگان و Pro موجود بوده که در این آموزش از نسخه رایگان آن استفاده شده است.

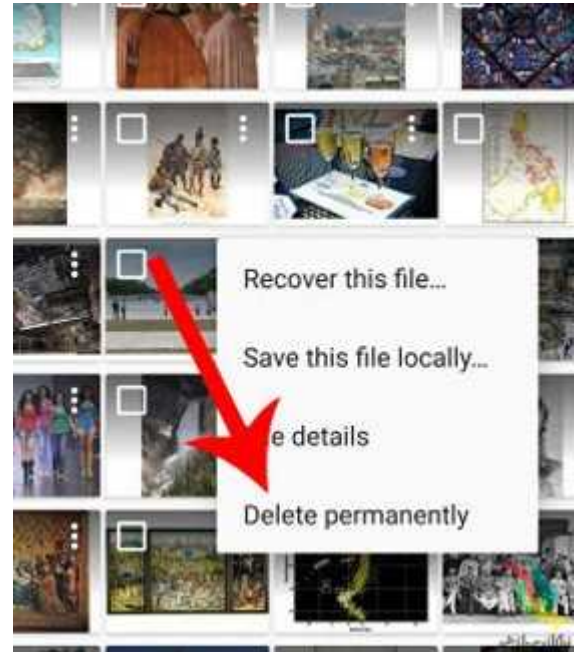
برنامه را باز کرده و روی START BASIC PHOTO SCAN کلیک کنید. با این کار تمامی تصاویر حذف شده‌ای که قابل بازگردانی هستند نمایان خواهند شد. دقت داشته باشید که اگر گوشی شما روت شده باشد، درصد خطای این برنامه در پیدا کردن تصاویر حذف شده، به حداقل خواهد رسید.



پس از مدتی انتظار، می‌توانید عکسهای حذف شده را مشاهده کنید. در این مرحله عکسهایی را که می‌خواهید به‌طور کامل از دستگاه شما پاک شوند، انتخاب کنید.



بر روی آیکون سه نقطه کلیک کرده و گزینه Delete Permanently را برگزینید.



در این حالت تصاویری که انتخاب کرده‌اید، به‌طور دائمی و بدون شانس بازگشت، پاک خواهند شد.

آیا اندروید به آنتی‌ویروس نیاز دارد؟



از همان ابتدای ورود دو سیستم عامل اندروید و iOS به بازار، بحث امنیت جزء لاینفک رقابت میان این دو بوده است. اپل و طرفدارانش همیشه روی امنیت بالای آیفون در مقابل گوشی‌های اندروید مانور داده و بدافزارهای اندرویدی را به‌عنوان شاهد مثال آورده‌اند!

این امر سبب شده عده زیادی اندروید را به مثابه ویندوز به همراه ویروس‌های متعددش ببینند و این سیستم عامل وجه خودش را در زمینه

امنیت در میان درصد قابل توجهی از کاربران از دست بدهد. بر این اساس، بسیاری این سوال در ذهنشان شکل گرفته که اندروید واقعا تا چه میزان امن است؟ آیا یک کاربر عادی اندروید باید نگران «ویروس» گرفتن گوشی یا تبلتش باشد و بنابراین به دنبال یک آنتیویروس خوب؟

پاسخ سوالات مطرح شده بنا به گفته مسئولان ارشد اندروید، منفی است. کمی پیش از کنفرانس سالانه گوگل در اوایل امسال، ایدرین لودویگ (Adiran Ludwig) مسئول امنیت اندروید به خبرنگاران اینطور گفته بود: «آیا من فکر میکنم کاربران عادی اندروید نیازی به نصب آنتیویروس دارند؟ قطعاً خیر. من فکر نمیکنم بیش از ۹۹ درصد کاربران نفعی از یک اپ آنتیویروس ببرند.» علاوه بر این، لودویگ معتقد است روی تهدیدات بدافزارهای اندروید زیادی تاکید شده است.

از سوی دیگر، شرکتهای امنیتی و سازندگان اپهای آنتیویروس برای اندروید چندان با این ادعا موافق نیستند. از نظر آنها ماجرا مانند بقال و ماست ترش میماند و گوگل قاعدتا هیچگاه به ایرادات فروشگاه پلیاستور و اپهای مشکوک در آن اعتراف نخواهد کرد، اما اجازه دهید قضیه را کمی دقیقتر بررسی کنیم.



انواع ویروسهای اندرویدی

در اصطلاح کامپیوتری، ویروس بهطور ساده نوعی برنامه مخرب است که خودش را بین دستگاههای مختلف تکثیر کرده و گسترش میدهد. این نوع برنامههای مخرب سالیان سال کاربران ویندوز را آزار داده و میدهد. در مورد اندروید نیز با توجه به محبوبیت و توسعه فوقالعاده آن، تهدیدات آن نیز رو به فراوانی گذاشته است. از نظر فنی نمیتوان به بدافزارهای اندروید ویروس گفت، زیرا امکان تکثیر ندارند، با این

وجود، این اصطلاح کماکان برای هر نوع بدافزاری به کار میرود.

در حالت کلی، بدافزارهای اندرویدی را میتوان در پنج نوع تقسیم کرد: دسته اول، کپی‌کارها هستند یعنی نرم‌افزارهای تقلبی هم‌شکل و هم‌نام بازی‌ها و نرم‌افزارهای مشهور که کاربران به اشتباه آنها را نصب می‌کنند. این بدافزارها پس از نصب، ممکن است اقدام به جمع‌آوری و ارسال داده‌ها یا استفاده از تبلیغات اپ‌های دیگر به نفع خود کنند. نرم‌افزارهای کرک‌شده نیز می‌توانند در این دسته قرار بگیرند.

دسته دوم، باج‌افزارها هستند که با قفل کردن دستگاه، سعی در اجبار کاربر به پرداخت مبلغی برای آزادسازی آن دارند!

دسته سوم، بدافزارهای رباینده (Hijacking) هستند. این بدافزارها با روش‌های مختلف مانند تبلیغات و نوتیفیکشن‌های فراوان به نحوی کنترل گوشی را از دست کاربر درمی‌آورند تا او به ناچار روی سایت یا تبلیغی که اپ می‌خواهد کلیک کند و گوشی آلوده شود.

دسته آخر نیز بدافزارهای فیشینگ (Phishing) هستند که با شبیه‌سازی صفحه ورود سایت‌های معتبر یا پیام‌هایی چون «اینجا کلیک کنید تا باتریتان افزایش یابد!» کاربر را به سمت ورود اطلاعات یا دانلود نرم‌افزارهای آلوده پیش می‌برند.

منشأ بدافزارهای اندرویدی

اصلی‌ترین و مهم‌ترین دروازه ورود بدافزارهای اندروید، منابع غیرمعتبر توزیع نرم‌افزار هستند. سایت‌هایی که انواع و اقسام نرم‌افزارهای پولی را به‌صورت رایگان قرار می‌دهند، دانلود فایل نصبی یک نرم‌افزار (apk) از تلگرام و دیگر شبکه‌های اجتماعی، مارکت‌های عجیب و غریب چینی و غیرچینی و مسیرهایی از این دست.

البته این به آن معنا نیست که در دیگر مارکت‌ها و حتی خود پلی‌استور بدافزار وجود ندارد. درصد زیادی از هکرها و برنامه‌نویسان این بدافزارها، از ایرادات امنیتی استفاده کرده و نرم‌افزارهایشان را به اشکال مختلف وارد پلی‌استور می‌کنند. گوگل نیز به‌طور مستمر این نرم‌افزارهای مشکوک را حذف و حفره‌های امنیتی کشف‌شده را می‌بندد، اما این روند در هر حال به‌صورت یک بازی موش و گربه پیش می‌رود!

بالاخره آنتی‌ویروس نصب کنم یا نه؟

پیش از آن‌که به فکر نصب آنتی‌ویروس بيفتيد، چند نکته امنیتی بسیار مهم وجود دارد که با رعایتشان در ردیف آن دسته کاربرانی قرار می‌گیرید که اصلاً نیازی به آنتی‌ویروس نخواهند داشت. اولین نکته آن است که مسیر ورودی بدافزارها را ببندید و تمام نرم‌افزارها و به‌روزرسانی‌هایشان را از پل‌استور یا مارکتهای معتبر داخلی دانلود کنید. هرگز سراغ دانلود و نصب نرم‌افزار از منبعی که نمی‌شناسید، نروید!

هنگام نصب و استفاده از نرم‌افزارها هم حواستان به درخواست اجازه‌های آنها باشد. اگر دیدید نرم‌افزاری درخواستی خارج از کارکرد متعارفش دارد یا از نصب آن خودداری کنید یا در نسخه‌های بالاتر اندروید، این اجازه را به آن ندهید.

نکته دوم، به روزرسانی خود اندروید است. در هر نسخه جدید اندروید، حفره های امنیتی بسیاری رفع می شود که امنیت گوشی شما را بالاتر می برد. بنابراین در داندلود و نصب نسخه جدید سیستم عامل گوشی تان شک نکنید!

نکته سوم ارتباطی به خود بدافزارها پیدا نمی‌کند، اما در هر صورت لازم است همیشه از داده‌های روی تلفن همراه‌تان بک‌آپ بگیرید و تا حد امکان از نگهداری داده‌های حساس روی آن خودداری کنید تا اگر اتفاقی چه نرم‌افزاری و چه سخت‌افزاری افتاد، فهرست نگرانی‌هایتان شامل از بین رفتن یا دزدی اطلاعات خصوصی نباشد!

حملاتی که به گوشی های هوشمند انجام میشود



تشریح نفوذ به یک دستگاه تلفن همراه

چگونه یک هکر می‌تواند از گوشی شما سوء استفاده کند؟

اندروید گوشی هوشمند شما ممکن است مبرا به نظر برسد، اما هنگامی که توسط بدافزارها مورد حمله قرار بگیرد متوجه می‌شوید که اطلاعات شما دیده و جعل می‌شود. شرکت در فعالیت های خودکار اینترنتی خطرناک است، و دزدیدن اطلاعات شخصی شما و حتی سرقت پول شما امکان دارد اتفاق بیافتد.



هزینه‌ی عنوان شده توسط محافظان اندروید در برابر برنامه‌های مخرب.



۱۱۳ گوشی هوشمند در آمریکا در هر دقیقه گم می‌شود.



۵.۴ میلیون دلار هزینه متوسط نگهداری از یک شعبه اطلاعات در سال ۲۰۱۲ در آمریکا بود.



۳۵۰۰۰۰ ویروس اندرویدی توسط Sophos Labs دیده شده است.