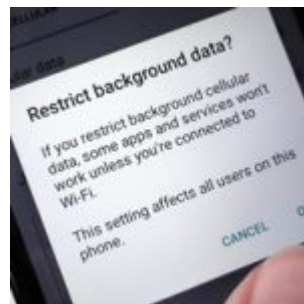


اعمال محدودیت دسترسی برنامه‌های اندرویدی به اینترنت

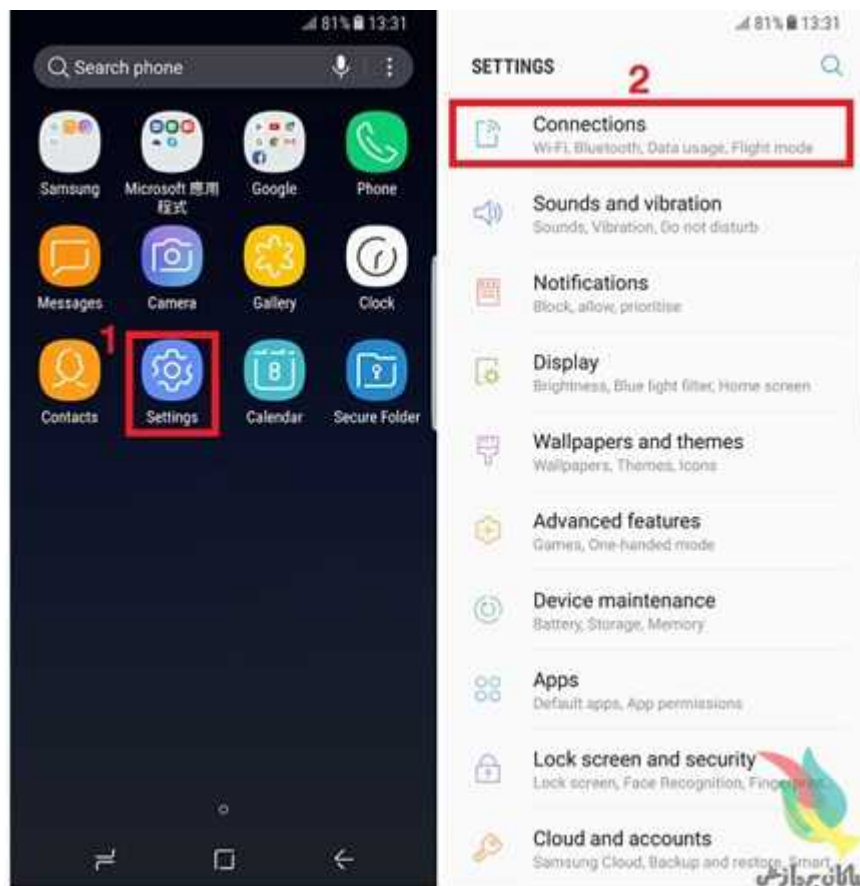


تاکنون چند مرتبه این اتفاق ناخوشایند را تجربه کرده‌اید که برنامه‌های کاربردی گوشی اندرویدی شما بدون اطلاع به اینترنت متصل شده‌اند، داده‌هایی را دریافت کرده یا ارسال کرده‌اند؟ ما در این مقاله راهکار جالبی را به شما معرفی می‌کنیم تا ضمن صرفه‌جویی در پهنای باند بتوانید مانع از آن شوید تا برنامه‌ها در پس‌زمینه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

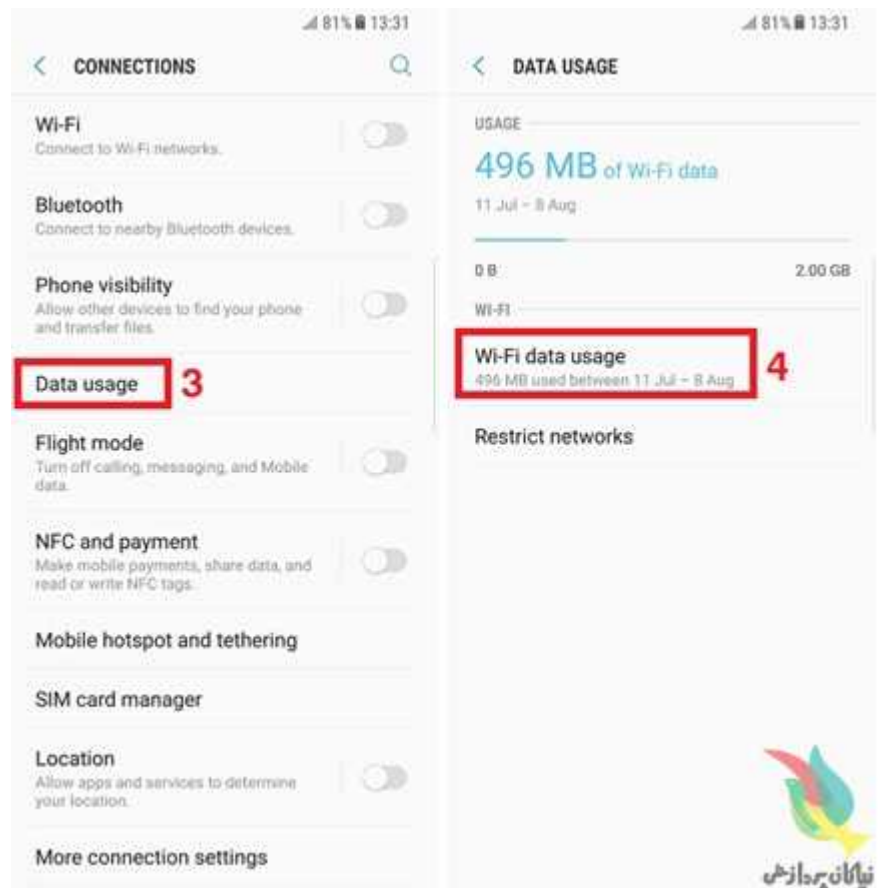
کاربران اندرویدی یک راهکار ساده اما ایده‌آل در اختیار دارند که به آن‌ها اجازه می‌دهد دسترسی برنامه‌های خاص به اینترنت را مسدود کنند. با توجه به این‌که امروزه برنامه‌های زیادی روی دستگاه اندرویدی شما نصب می‌شوند، جای تعجب نیست که بسیاری از این برنامه‌ها بدون اطلاع شما به اینترنت متصل شوند. این اتفاق از 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

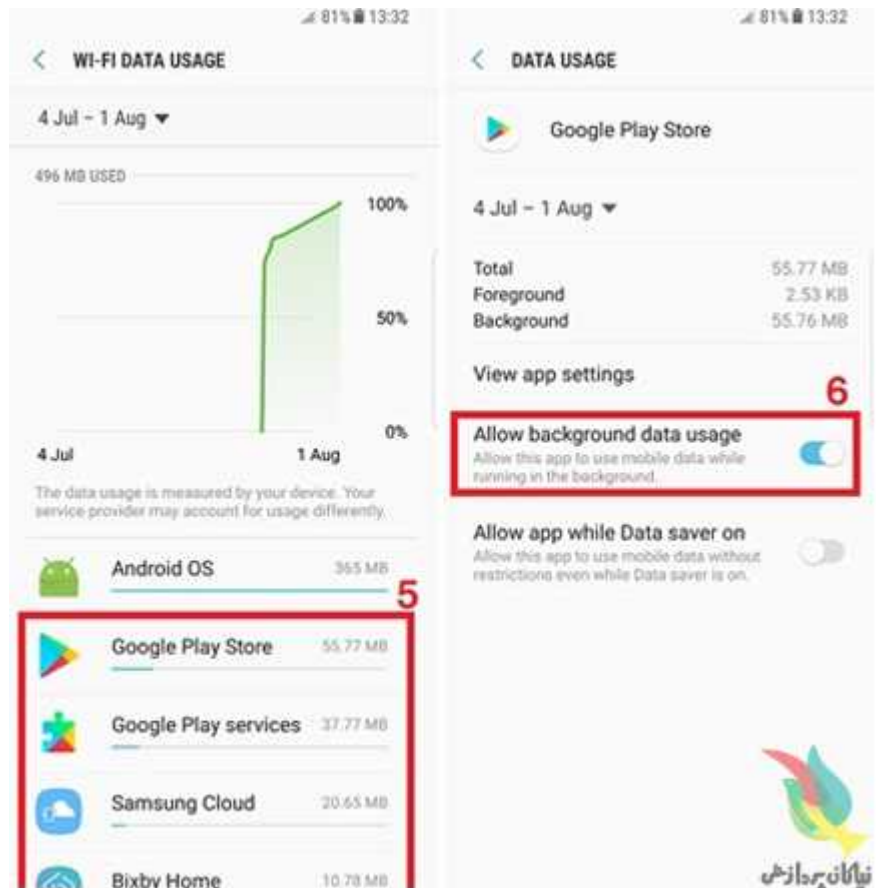
گام اول، در گوشی اندرویدی (سامسونگ) به بخش Settings بروید. اکنون گزینه Connections را انتخاب کنید.



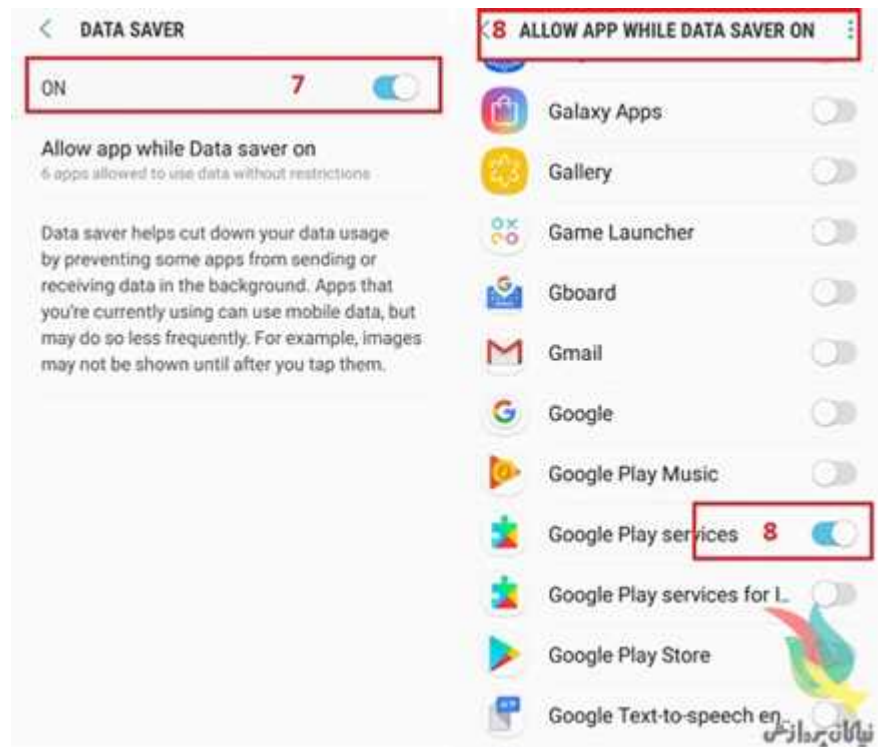
گام دوم، اکنون گزینه Data usage را انتخاب کرده و در ادامه گزینه Wi-Fi data usage را انتخاب کنید.



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

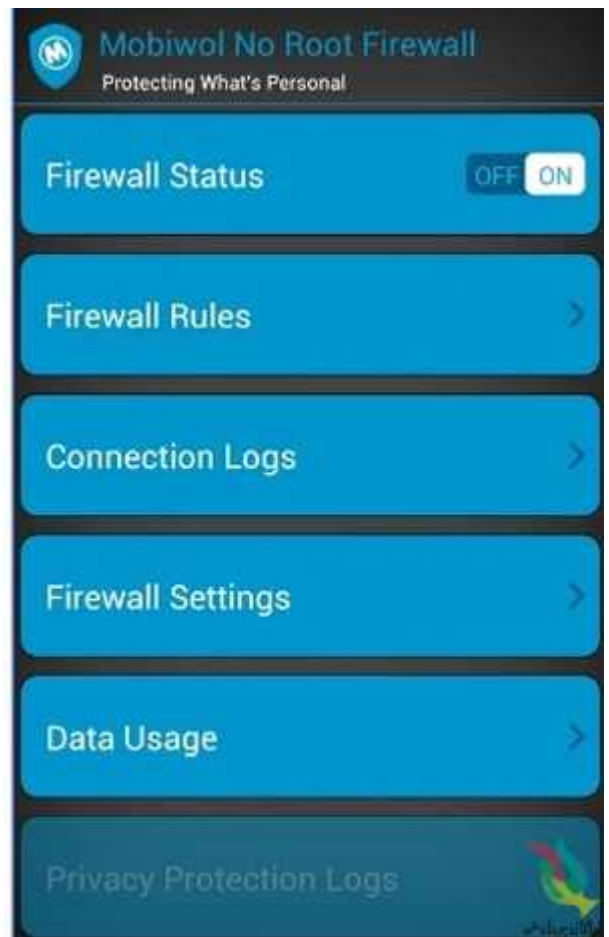
گام اول، ابتدا برنامه Mobiwol را از فروشگاه گوگل پلی دانلود کرده و روی گوشی خود نصب کنید

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

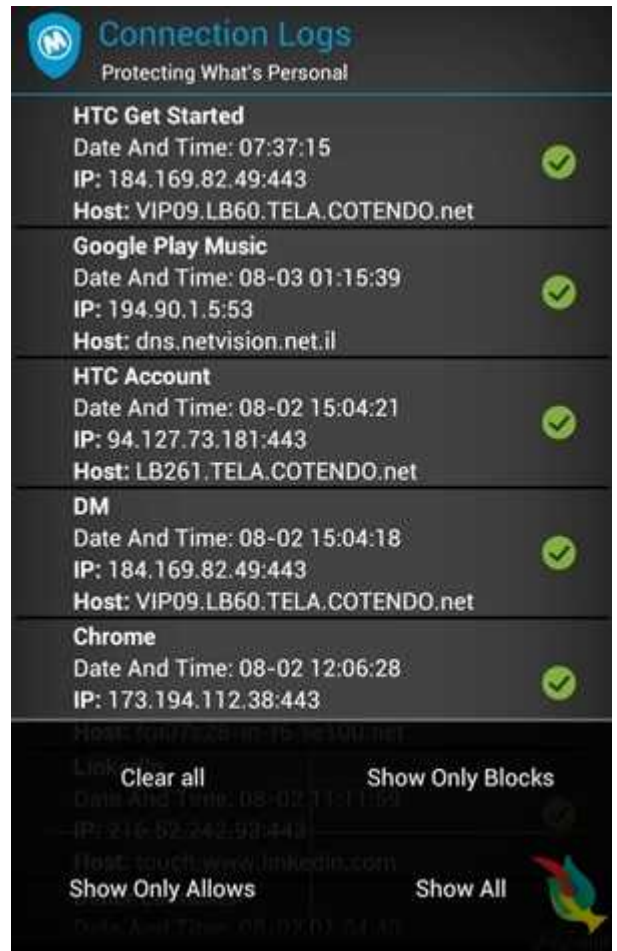
گام سوم، اکنون فهرستی از برنامه‌های کاربردی که روی گوشی شما نصب شده‌اند را مشاهده می‌کنید. در مقابل هر کدام از این برنامه‌ها دو گزینه وجود دارد. یکی از این گزینه‌ها اجازه دسترسی به وای‌فای و دیگری اجازه دسترسی به اینترنت موبایلی در پس‌زمینه دستگاه را به برنامه کاربردی تخصیص می‌دهند.



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.

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 بیفتید، 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 پلی‌استور 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، به‌روزرسانی خود اندروید است. در هر نسخه جدید اندروید، حفره‌های امنیتی بسیاری رفع می‌شود که امنیت گوشی شما را بالاتر می‌برد. بنابراین در دانلود و نصب نسخه جدید سیستم‌عامل گوشی‌تان 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!

این ۱۲ کار را با گوشی

اندرویدی تان انجام ندهید!



گوشی‌های اندرویدی از پر مصرف ترین ابزارهای کنونی در میان مردم به حساب می‌آیند، یک ابزار همیشه آماده و همه کاره که در قالب تلفن همراه قرار گرفته ولی تنها یکی از هزاران کاری که با آن انجام می‌دهیم برقراری تماس است!



اینبار برایتان از کارهایی می‌نویسیم که انجام دادن آنها خواهد توانست به شما و گوشی اندرویدیتان آسیب وارد کند! با ما همراه باشید:

حتما بر روی گوشی قفل بگذارید!

رسم پترن‌ها یا رمزهای چند رقمی یا پین کد از مرسوم ترین روش‌هایی است که به واسطه آنها می‌توانیم گوشی موبایل را از هرگونه سرقت اطلاعات در مراحل اولیه محافظت کنیم. حتما و بدون شک این مورد پیشنهاد می‌شود و فراموش نکنید که حتما رمزی را انتخاب کنید که فراموش کردنش برایتان دشوار باشد!

همیشه به روز باشد!

تا همین چند وقت پیش (یکی دو سال پیش) بروز رسانی در دستگاه‌های

اندرویدی یک رویا به حساب می‌آمد! اما اکنون به لطف توسعه اندروید در نسخه‌های بالاتر و سعی کوشش شرکت‌های تولید کننده شاهد بروز رسانی‌های به موقع و زمان‌بندی شده برای دستگاه‌های اندرویدی هستیم. حتماً بروز رسانی‌هایی که در اعلان‌هایتان دریافت می‌کنید را دانلود و نصب کنید! این کار هم سرعت دستگاه شما را بالاتر خواهد برد و هم در امنیت شما تاثیر بسزایی خواهد داشت.

با کابل usb گوشی را شارژ نکنید!

همانطور که میدانید اتصال گوشی اندرویدی به کامپیوتر با کابل usb همزمان در حین انتقال اطلاعات گوشی شما را نیز شارژ خواهد کرد! توجه کنید که این کار باعث شارژ گوشی شما خواهد شد، اما چون همانند شارژر خود دستگاه امکان تامین انرژی مورد نیاز را ندارد به مرور به سیستم انتقال قدرت و باتری دستگاه شما آسیب خواهد رسید! پس از تکرار این کار پرهیز کنید.

تهیه بک آپ را فراموش نکنید!

هر از گاهی گوشی را به کامپیوتر متصل کنید و از اطلاعاتتان بک آپ تهیه کنید. تصاویر، فیلم‌ها و سایر فایل‌های مهم را در جایی دیگر هم ذخیره کنید، بدون شک از انجام متداول این کار پیشمان نخواهید شد!

زیاد به کلودها اطمینان نکنید!

سیستم‌های ابری فراوانی در حال حاضر فعال هستند و اطلاعات ما را با اجازه ما ثبت و ضبط می‌کنند. توجه داشته باشید زیاد هم متکی به این امکانات نباشید! این اتفاق بعید است اما در صورتی که تنها به این فضاهای ذخیره سازی بسنده کنید احتمال اینکه در لحظه نتوانید به اطلاعات مهمتان درست یا بید کم نیست! اختلال در خطوط، از دسترس خارج شدن سرور، فیلترینگ و ...

داغ شدن گوشی به باتری و برد اصلی دستگاه آسیب جدی وارد می‌کند

نگذارید گوشی‌تان زیاد داغ کند!

با انجام بازی‌های سنگین، یا اتصال طولانی مدت به اینترنت وایرلس یا استفاده از دیتا و یا باز بودن همزمان چندین برنامه معمولاً دما دستگاه تا حد بسیار زیادی بالا می‌رود! این اتفاق را با گرم شدن در دست گوشی متوجه می‌شویم. سعی کنید از داغ شدن و داغ ماندن دستگاه

جلوگیری کرده و حتما دستگاه را به حال خودش رها کنید. اگر کیس یا همان قاب گوشی روی دستگاه نصب دارید آن را حتما جدا کنید. داغ شدن گوشی باعث اورهیت شدن شده و بدون شک به سیستم انتقال قدرت، باتری و برد اصلی دستگاه آسیب جدی وارد می‌کند.

صفحه گوشی را با محافظ دریا بید!

نام gorilla glass را حتما شنیده اید، این عنوان نام تکنولوژی به کار گرفته شده در صفحه‌های نمایشگر است و صفحه نمایش گوشی‌ها را از هرگونه آسیب محافظت می‌کند. اما توجه داشته باشید طبق امتحان‌هایی که صورت گرفته و بر حسب تجربه، گران‌ترین و بروزترین گوشی‌ها هم بعد از مدتی استفاده بدون محافظ دچار آسیب روی صفحه نمایش می‌شوند! حتما و بدون تردید از محافظ صفحه نمایش استفاده کنید.

زیاد روی ضدآب بودن حساب باز نکنید!

گوشی‌ها جدید همگی از این استانداردها طبیعت می‌کنند. توصیه اکید ما این است که حتی الامکان مراقب گوشی باشید و در مقابل گرد و غبار و آب از آن محافظت کنید! به خاطر داشته باشید، در صورت هرگونه آسیب هیچ یک از گارانتی‌های موجود در بازار جوابگوی شما نخواهند بود، پس حتما خودتان از هرگونه مشکل پیشگیری کرده و از آب خوردگی دستگاه پرهیز کنید.

عکس‌ها و ویدئو را مدیریت و آرشیو کنید!

این مورد را در بالا هم گفتیم. اکنون تاکید می‌کنیم که حتما تصاویر موجود از سلفی‌ها و هر مورد شخصی را به کامپیوتر شخصی خودتان منتقل کرده و تعداد تصاویر موجود در گوشی را به حداقل برسانید! بدون شک از انجام این کار پشیمان نخواهید شد!

سنسورهای بی مورد را روشن نگذارید!

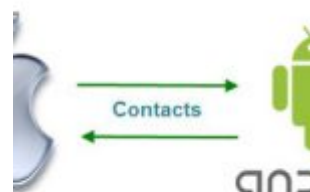
گوشی‌های کنونی همگی از سنسورها و چیپ‌های مختلفی بهره می‌برند، توجه کنید که روشن بودن آنها باعث مصرف باتری دستگاه شده و اجرای برنامه‌ها را با کند بودن همراه می‌کند! موارد اضافی را مثل gps، nfc بلوتوث و ... را در مواقعی که کاری با آنها ندارید خاموش نگاه دارید. برای اینکار کافی است نوار اعلان‌های بالا صفحه را پایین کشیده و آیکون‌های روشن را خاموش کنید!

اپ‌های بی نام و نشان را نصب نکنید!

به لطف پیشرفت اندروید تعداد بسیار زیاد شده است و برای هر کاری که فکرش را هم نمیکنید اپ خواهید یافت. لطفاً از نصب اپ‌های بی‌هوده و بی‌نام و نشان بپرهیزید و همین الان اگر آنها را روی دستگاهتان دارید حذف کنید. بسیاری از این اپ‌ها بدون اجازه شما به اطلاعاتتان دسترسی خواهند داشت و در بهترین حالت باعث کندی بی‌مورد و نمایش تبلیغات در صفحه گوشی خواهند شد.

منبع: بیتوته

سه روش ساده برای انتقال مخاطبان از آیفون به اندروید



انتقال شماره مخاطبین از آیفون به اندروید مشکل بسیاری از کاربران دستگاه‌های هوشمند است.



در این مطلب می‌توانید سه روش ساده برای انتقال مخاطبان از آیفون به اندروید را در دستگاه هوشمند خود امتحان کنید. برای انجام این

کار کافیسٹ طبق مراحل زیر عمل کنید.

روش اول

ایجاد یک حساب کاربری گوگل است که از طریق سایت گوگل و انتخاب گزینه create account امکان پذیر خواهد بود، پس از ایجاد اکانت، به قسمت تنظیمات آیفون رفته و گزینه های Mail، Contacts و Calendars را انتخاب کنید، پس از ورود به این بخش بر روی add کلیک کرده و با انتخاب جیمیل مشخصات اکانتی که ساخته اید را وارد کنید.

پس از اطمینان از اتصال به اینترنت آیفون در این قسمت از شما سوال می پرسد که چه قسمتی از اکانت را با موبایل همگام کند باید خواستان باشد که گزینه کانتکت فعال باشد، پس از اطمینان از این قسمت همگام سازی بین اندروید و آیفون آغاز می شود و ممکن است کمی طول بکشد.

روش دوم

استفاده از iCloud است، این برنامه سرعت بیشتری برای انتقال لیست مخاطبان دارد، در آیفون قسمت تنظیمات مجدد سه گزینه ای که اشاره شده را به ترتیب بفشارید و در قسمت اکانت بروید تا گزینه iCloud را مشاهده کنید، تیک گزینه کانتکت را بزنید، در این مرحله آیفون از شما می خواهد که لیست مخاطبان شما با iCloud ادغام شود، به سایت iCloud بروید اپل آی دی خود را وارد کنید و گزینه کانتکت را فعال کرده و همه مخاطبان را نشانه دار کنید و سپس Export vCard را فعال نمایید.

در مرحله بعد در این روش جیمیل خود را باز کنید، Contacts و سپس Import ، More و Choose File را فعال کنید، فایلی که از قبل ذخیره شده را انتخاب کنید، پس از اتمام کار لیست مخاطبان شما نشان می دهد.

روش سوم

استفاده از اپلیکیشن iTunes است، برای استفاده از این اپلیکیشن باید آیفون خود را به سیستم کامپیوتری متصل کنید، اپلیکیشن یاد شده را باز کنید و گزینه آیفون را در بالای iTunes انتخاب نمایید، با گزینه info و سپس فعال کردن Sync Contacts with و انتخاب

Google Contacts نیمی از راه انتقال را پیموده اید، حالا باید مشخصات اکانت گوگل را وارد کنید تا همگام سازی به پایان برسد و مخاطبانتان را در اندروید ببینید.

منبع: بیتوته