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 نمی شود . 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 می آورند و فکر می کنند اطلاعات گوشی شان پاک می شود اما باید بدانید نرم افزار هایی وجود دارد که امکان بازیابی اطلاعات گوشی را به شما می دهد حتی بعد از ریست فکتوری .برای جلوگیری از دسترسی به اطلاعات گوشی باید آنها را رمگذاری 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
تلفتن 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 بازنوشته 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 متاسفانه 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 می کند، بازیابی اطلاعاتی است که به خیال آن ها حذف
شده است و یکی از بزرگ ترین مشکلات به خطر افتادن حریم شخصی افراد می باشد و برای جلوگیری از
چنین رخدادی راه حلی وجود دارد.

رمزگذاری تلفن همراه و سپس بازگشت به تنظیمات کارخانه

رمزگذاری، مطمئن ترین راه برای جلوگیری از بازیابی اطلاعاتی است که فکر می کنید حذف شده اند.
با این روش شما اطلاعات خود را قفل می کنید و فقط با وارد کردن کلماتی که شما آن ها
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؟

گوشی هایی که سیستم عامل آن ها مجهز به اندروید ۶ هستند، نیازی به این تنظیمات ندارند و توسط شرکت
گوگل به طور اجبار رمز گذاری می شوند و بیشترین ضریب امنیتی را دارند و دسترسی به آن ها کار
آسانی نیست.
اما اگر سیستم عامل شما مجهز به اندروید ۵ به پایین است، می توانید با استفاده از شیوه زیر، از
امکان رمزگذاری روی اطلاعات در گوشی خود استفاده کنید.

نکته قابل ذکر این است که فقط برخی از تلفن های همراه از چنین قابلیتی 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 بازنوشته 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 متاسفانه برخی ابزارهای بازیابی فایل وجود دارند که می‌توانند این نوع فایل‌های 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 خو 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 داده‌اید 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 می توانید 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 رمزی داشته باشد، در این مرحله از شما پرسیده خواهد شد
تا از ریست شدن دستگاه به دست دیگران جلوگیری شود.

منبع:persianv.com

چطور اکانت اینستاگرام خود را در حالت خصوصی (Private) قرار دهیم؟

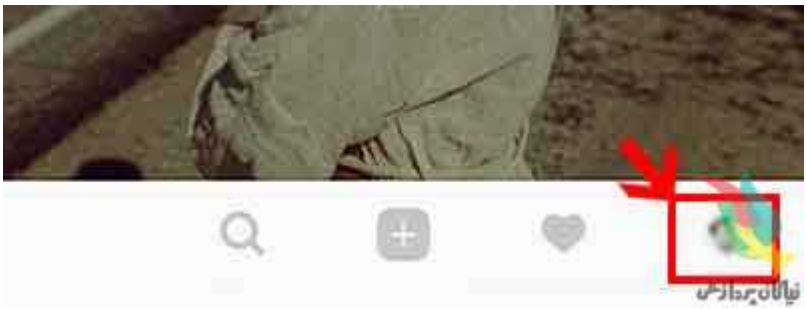
اینستاگرام این امکان را به کاربر می‌دهد تا اکانت کاربری خودش را در دو حالت خصوصی و عمومی داشته باشد و بدین ترتیب با کنترل بیشتر حسابش را مدیریت کند. در این مطلب نحوه خصوصی کردن حساب اینستاگرام (اکانت اینستاگرام Private) را آموزش می‌دهیم. همراه ما باشید.

اکانت شما در اینستاگرام می‌تواند در حالت عمومی و یا خصوص قرار بگیرد که هر کدام ویژگی‌های خاص خودشان را دارند. در حالت خصوصی یا Private، افراد ناشناسی که در فالوورهای شما نیستند، به اکانت‌تان دسترسی نخواهند داشت و پس از درخواست و تایید شما، به لیست فالوورهای‌تان اضافه می‌شوند. این دسته از افراد پس از طی این مرحله قادر به مشاهده حساب کاربری شما خواهند بود.

در صورتی که اکانت اینستاگرام خود را در حالت عمومی یا Public قرار دهید، دسترسی همه افراد به حساب کاربری‌تان آزاد بوده و بدون نیاز به فالو کردن، می‌توانند پست‌های مختلف شما را مشاهده کنند.

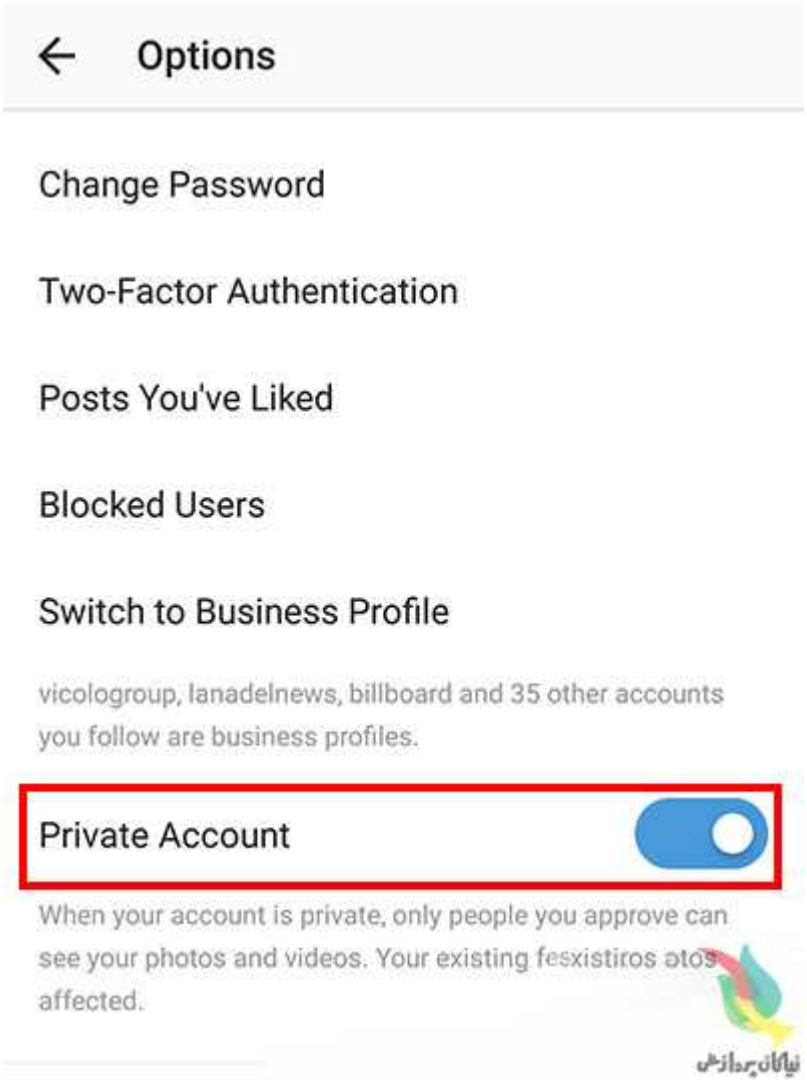
در صورتی که از عمومی بودن اکانت کاربری خود ناراضی هستید، در این مطلب نحوه خصوصی کردن حساب اینستاگرام را به شما آموزش می‌دهیم. برای این کار مراحل زیر را به ترتیب دنبال کنید.

اپ اینستاگرام را باز کرده و وارد پروفایل شخصی خود شوید.



بر روی آیکون آپشن که به صورت سه نقطه در بخش بالایی رابط قرار گرفته، کلیک کنید.

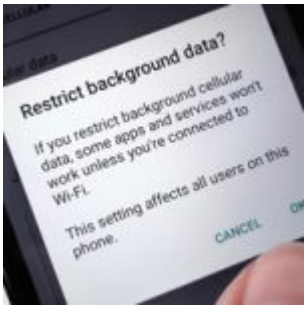
به بخش Account رفته و گزینه Private Account را فعال کنید.



با پایان این مراحل حساب کاربری اینستاگرام شما در حالت خصوصی یا همان Private قرار گرفته و کاربران ناشناس برای دسترسی به پست‌های شما، باید به شما در خواست فالو بدهند. برای بازگردانی حساب کاربری به حالت عمومی کافی است همین مراحل را یک بار دیگر طی کنید و گزینه Private Account را غیر فعال کنید. دقت کنید با این کار تمامی درخواست‌های فالوی شما که در زمان خصوصی بودن اکانت ارسال شده بود، تایید شده و آن افراد به صورت خودکار به لیست فالوورهای‌تان اضافه می‌شوند.

منبع: بیتوته

اعمال محدودیت دسترسی برنامه‌های اندرویدی به اینترنت

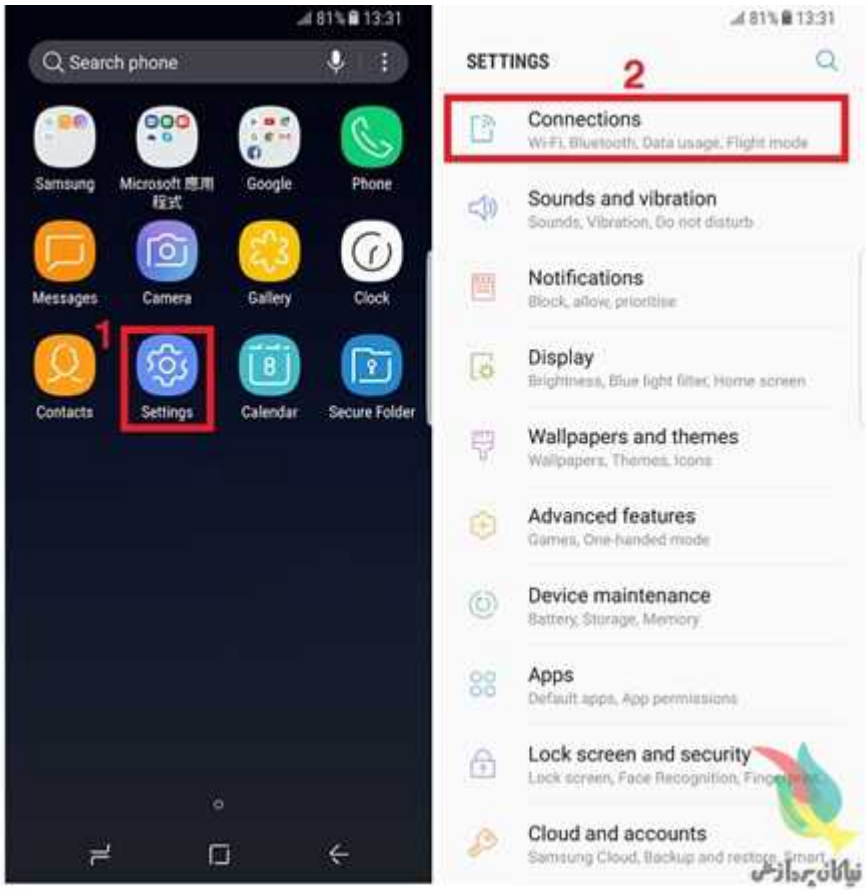


تاکنون چند مرتبه این اتفاق ناخوشایند را تجربه کرده‌اید که برنامه‌های کاربردی گوشی اندرویدی شما بدون اطلاع به اینترنت متصل شده‌اند، داده‌هایی را دریافت کرده یا ارسال کرده‌اند؟ ما در این مقاله راهکار جالبی را به شما معرفی می‌کنیم تا ضمن صرفه‌جویی در پهنای باند بتوانید مانع از آن شوید تا برنامه‌ها در پس‌زمینه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

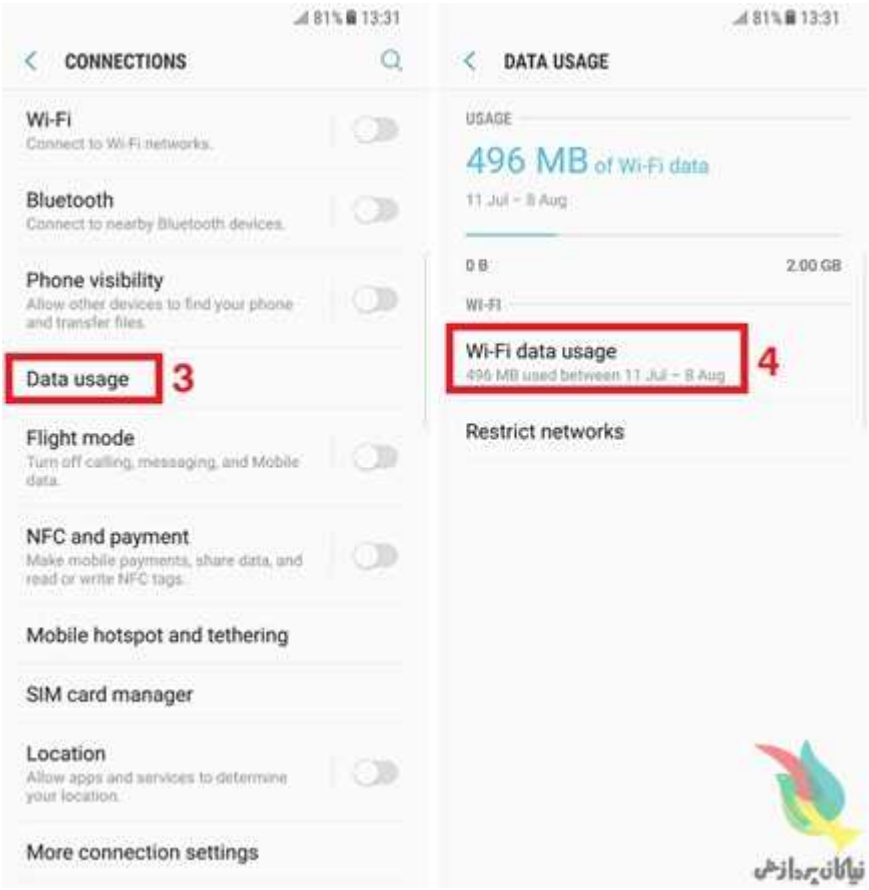
کاربران اندرویدی یک راهکار ساده اما ایده‌آل در اختیار دارند که به آن‌ها اجازه می‌دهد دسترسی برنامه‌های خاص به اینترنت را مسدود کنند. با توجه به این‌که امروزه برنامه‌های زیادی روی دستگاه اندرویدی شما نصب می‌شوند، جای تعجب نیست که بسیاری از این برنامه‌ها بدون اطلاع شما به اینترنت متصل شوند. این اتفاق از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

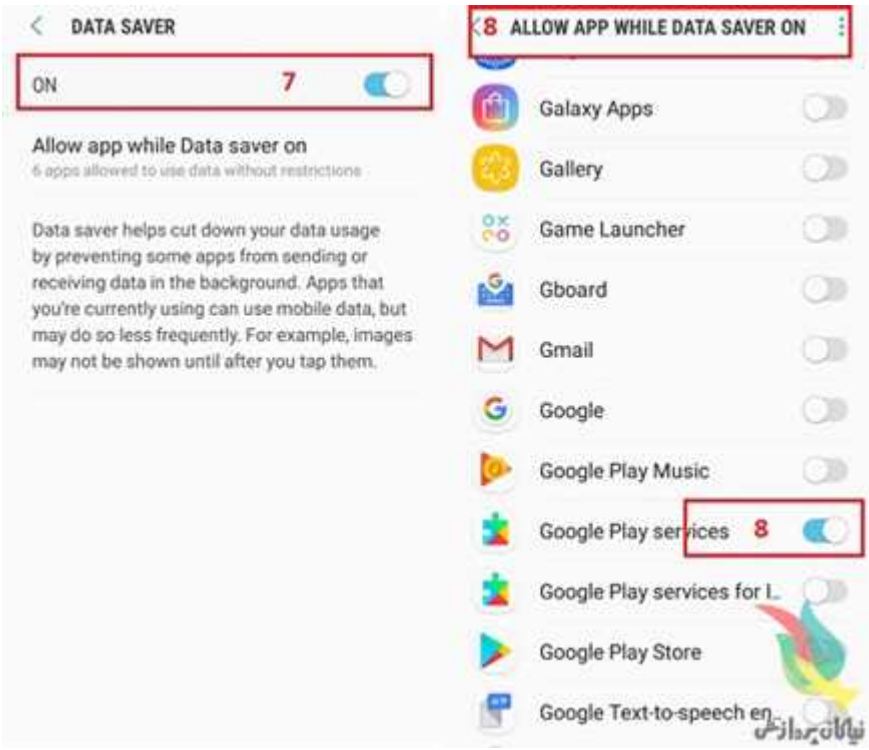


گام دوم، اکنون گزینه Data usage را انتخاب کرده و در ادامه گزینه Wi-Fi data usage را انتخاب کنید.



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، به‌کارگیری برنامه‌های ثالث

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

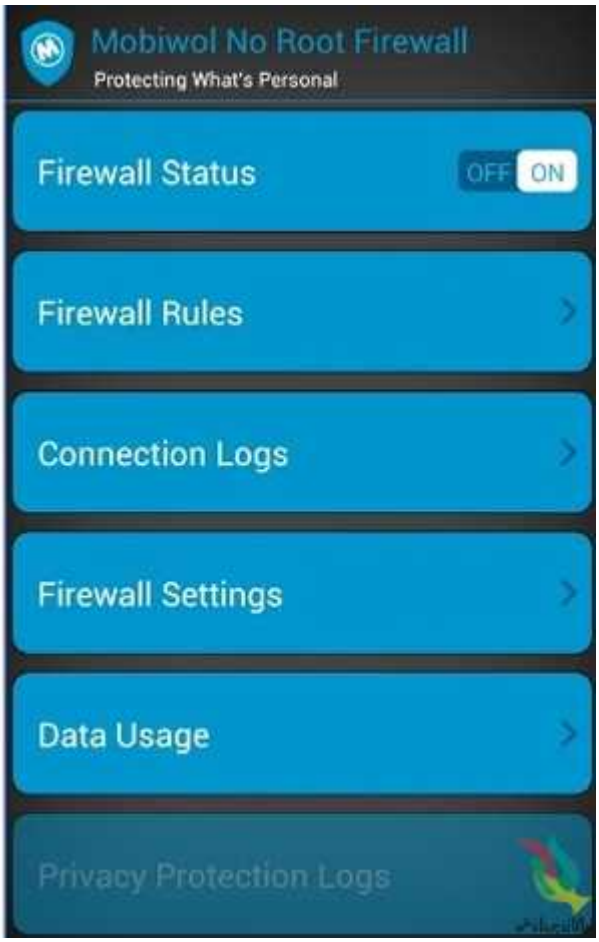
Mobiwol: بدون نیاز به روت کردن دستگاه

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

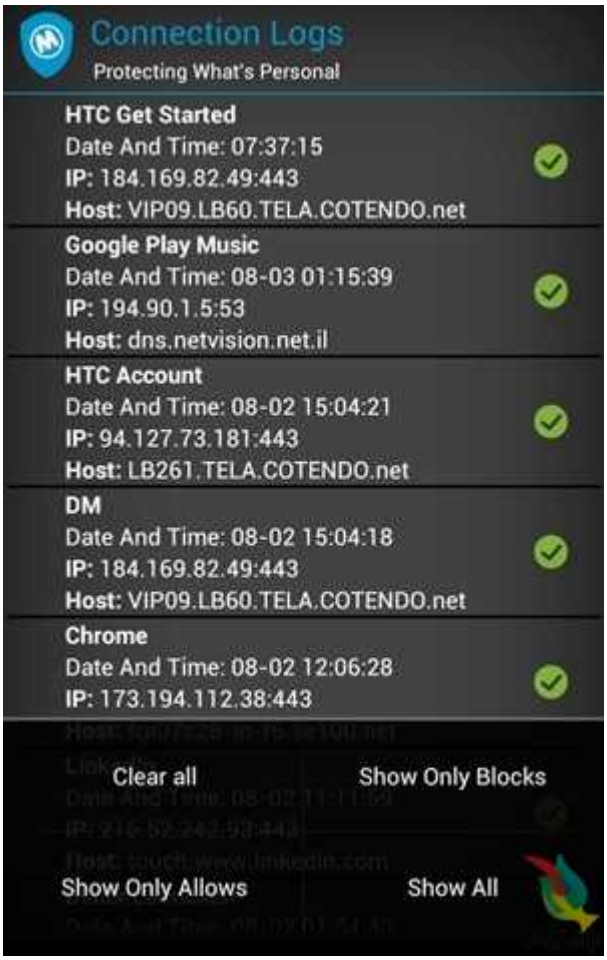
گام دوم، برنامه را اجرا کنید. با این‌کار گزینه به نام Firewall Rules را مشاهده می‌کنید. آن‌را لمس کنید.

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.

دسترسی به عکسهای پاک شده در تلفن‌همراه

برخلاف تصور شما عکسهای پاک شده در تلفن‌همراه‌تان به‌راحتی قابل دسترسی‌اند!

دسترسی دوباره به عکس‌هایی که از تلفن هوشمندتان پاک می‌کنید، بسیار آسان بوده و همین موضوع می‌تواند گاهی اوقات بسیار مشکل‌ساز باشد.

برای مثال حالتی را در نظر بگیرید که می‌خواهید گوشی خود را که صدها عکس شخصی در آن ذخیره کرده‌اید، بفروشید. در این وضعیت خیلی راحت وارد گالری می‌شوید 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؟

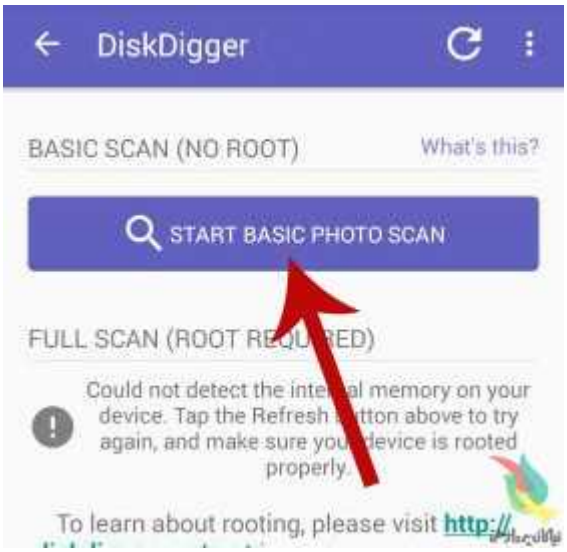
در واقع شما باید با انجام عملیاتی، عکس‌ها را به‌صورتی پاک کنید که در آینده با هیچ روشی قابل بازگردانی نباشند.

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 می خواهید 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 دایمی و بدون شانس بازگشت، پاک خواهند شد.

آیا اندروید به آنتی‌ویروس نیاز دارد؟

از همان ابتدای ورود دو سیستم‌عامل 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 سیستم‌عامل 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؟ قطعا 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 اصلا 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 حدامکان 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!

چه تفاوتی بین علامت های H+، H، G، E، ۳G و ۴G در اینترنت همراه وجود دارد؟

آیا تاکنون به علامت های مختلف G، E، ۳G، H، H+ و ۴G که در گوشی های هوشمند و نوار وضعیت آن ها مشاهده می شود توجه نموده اید و یا از خود پرسیده اید که چه تفاوتی بین این علامت ها وجود دارد؟

در واقع هر یک از این علامت ها نشان می دهد که شما به چه نوع از شبکه داده ها وصل شده اید ، و این شبکه های مختلف با توجه به علامت آن ها ، امکانات و سرعت اتصال به اینترنت بسیار متفاوتی ارائه می کنند.

معرفی نسل های اینترنت همراه

G – GPRS

جی پی آر اس ، مخفف عبارت General Packet Radio Service می باشد که با نماد G در گوشی های هوشمند قابل مشاهده می باشد.به این سرویس ، اینترنت نسل دوم نیز می گویند که سرعت تبادل اطلاعات آن چیزی در حدود ۱۱۵ کیلوبیت بر ثانیه (معادل ۱۴ کیلوبایت بر ثانیه) می باشد.

E – EDGE

اِج مخفف عبارت ، Enhanced Data Rates for GSM Evolution می باشد که مانند GPRS در نسل دوم شبکه های تلفن همراه قرار دارد با این تفاوت که سرعت دریافت اطلاعات در آن بیشتر و در حدود ۴۸ کیلوبایت بر ثانیه می باشد.
به EDGE نسل ۲٫۵G نیز گفته می شود و در تلفن های همراه با نماد E قابل مشاهده می باشد.

۳G

نسل سوم تلفن همراه که به تازگی در ایران ارائه شده است ، ۳G نام دارد که مخفف عبارت UMTS می باشد. سرعت انتقال داده در این نسل حدود ۳۹۵ کیلوبایت بر ثانیه می باشد و امکان برقراری تماس تصویری نیز یکی از قابلیت های این نسل می باشد.

H – HSDPA

اچ اس دی پی ای نسخه کمی کندتر HSDPA + می باشد که سرعت انتقال داده ی آن چیزی در حدود ۱٫۷۵ مگابایت برثانیه می باشد.با استفاده از این نسل می توان ویدئو های موجود در اینترنت را با وضوح HD به راحتی مشاهده کرد.
این نسل براساس ۳G کار می کند و گاها به این نسل ۳٫۵G نیز گفته می شود. در گوشی های همراه HSDPA با نماد H قابل مشاهده می باشد.

H+ – HSDPA Plus

نسل HSDPA+ نسخه سریع تر HSDPA می باشد که سرعت دریافت داده ها در این نسل ، حدود ۲۱ مگابایت بر ثانیه می باشد.
نسل HSDPA Plus در تلفن های همراه با نماد H+ نشان داده می شود.

۴G – LTE

۴ جی نسل چهارم شبکه های تلفن همراه می باشد که در حال حاظر سریع ترین و جدیدترین نسل این شبکه ها می باشد.سرعت دریافت داده در این نسل حدود ۳۷ مگابایت برثانیه می باشد.

اینترنت نسل پنجم یا ۵G چیست؟

در حال حاضر شبکه‌ی LTE و در برخی نقاط دنیا شبکه‌ی LTE-A متداول است. اهداف نسل بعدی که نام بسیار ساده‌ای دارد، توسط اتحادیه‌ی شبکه‌های همراه تدوین شده و شامل موارد زیر است:

- سرعتی در حد چند ده مگابایت بر ثانیه (برای ده ها هزار کاربر)
- اینترنت ۱ گیگابیت بر ثانیه ای برای ۱۰ کارمندی که در یک دفترکاری مشغول فعالیت هستند.
- چندصد هزار کانکشن یا مسیر ارتباطی برای اتصال شبکه‌ای عظیم از حسگرها به اینترنت (در اینترنت اشیاء و وسایل هوشمند)
- بازدهی شبکه بایستی به مراتب بهینه‌تر از ۴G باشد؛ به عبارت دیگر بتوان از پهنای باند موجود، استفاده‌ی کامل‌تری کرد.
- پوشش بهینه تر باشد.
- بازدهی سیگنال دهی افزایش یابد.
- تأخیر شبکه به مراتب کمتر از شبکه‌ی ۴G باشد.

در میان موارد فوق، حداقل سرعت ۱ گیگابیت بر ثانیه که چند برابر بیشتر از سرعت LTE است، تأخیر زیر ۱ میلی‌ثانیه و مصرف انرژی بهینه‌تر، بسیار مهم هستند. در حقیقت شبکه‌ی ۵G تنها برای تجربه‌ی سرعت بالاتر معرفی نمی‌شود بلکه قرار است وسایل هوشمند منزل، محیط کار و شهر را وارد شبکه‌ای بزرگ و گسترده کند.

منبع: مقداد آی تی

حذف فایل‌های تکراری در گوشی‌های هوشمند

معمولاً همه ما در گوشی‌های هوشمند خود فایل‌های زیادی را نگه داری می‌کنیم. برخی از این فایل‌ها تکراری هستند و فضای زیادی از گوشی ما را اشغال می‌کنند. بررسی تک‌تک فایل‌های ذخیره شده بر روی گوشی، و پیدا کردن فایل‌های تکراری و حذف آنها کار آسانی نیست و بسیار وقت گیر است. ما در این مقاله آموزشی به شما اپلیکیشنی را معرفی می‌کنیم که این کار را برای شما به آسانی انجام می‌دهد.

اپلیکیشن Duplicate Files Fixer، اپلیکیشن مناسبی است که به آسانی و با سرعت بالا فایل‌های موجود در گوشی شما را اسکن می‌کند، فایل‌های تکراری را شناسایی و حذف می‌کند. این اپلیکیشن به شما کمک می‌کند از شر فایل‌های تکراری و بی‌مصرف خلاص شوید و فضایی از حافظه گوشی شما را آزاد می‌کند.

اپلیکیشن Duplicate Files Fixer، فایل‌ها با محتویات عکس، ویدیو، اسناد که در گوشی شما ذخیره است را اسکن می‌کند و لیست فایل‌های تکراری را برای شما نمایش می‌دهد و پس از آن با تایید و انتخاب شما آنها را به آسانی پاک می‌کند.

این اپلیکیشن ویژگی‌های کاربردی دارد که شما به آسانی می‌توانید آن را به صورت رایگان از گوگل‌پلی دانلود و استفاده نمایید. استفاده از این اپلیکیشن در آزاد کردن فضای حافظه گوشی شما تاثیر بسزایی دارد.

بعد از دانلود برنامه از گوگل‌پلی و اجرا کردن آن برای بار اول این اپلیکیشن از شما مجوز دسترسی به فایل‌های موجود در گوشی با محتویات‌های مختلف را می‌خواهد. پس از صدور مجوز دسترسی اپلیکیشن به این بخش‌ها، در گام بعدی شما باید انتخاب کنید که کدام دسته از فایل‌های موجود در گوشی شما را اسکن کند، مثلاً فایل عکس‌ها را می‌توانید انتخاب کنید، تا عکس‌های تکراری را از میان آنها برای

شما شناسایی کند. شما می‌توانید گزینه Full Scan هم انتخاب کنید. با انتخاب این گزینه این اپلیکیشن کلیه فایل‌های موجود در گوشی شما را به منظور پیدا کردن فایل‌های تکراری اسکن می‌کند.

پس از مدت کوتاهی نتیجه اسکن فایل‌ها را برای شما نمایش می‌دهد. شما می‌تواند از فایل‌های تکراری یکی را انتخاب کنید و برای حذف آن گزینه Delete Now را فشار دهید (این کار می‌تواند به صورت گروهی هم انجام شود، یعنی تیک فایل‌هایی که می‌خواهید آنها را پاک کنید، را بزنید و پس از آن گزینه Delete Now را انتخاب کنید تا همه فایل‌ها به صورت یکجا و با هم پاک شود).

به همین سادگی و تنها با نصب اپلیکیشن Duplicate Files Fixer بر روی گوشی خود، می‌توانید از شر فایل‌های تکراری گوشی خود خلاص شوید.

منبع: بیتوته

این ۱۲ کار را با گوشی اندرویدی‌تان 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 رقمی‌ویا 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. حتما 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 یابید کم نیست! اختلال در خطوط، از دسترس خارج شدن سرور، فیلترینک 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 معمولا 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 مانند 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 دریابید!

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، گران ترین 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 طبعیت 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 هر گونه 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.

عکس‌هایتان را مدیریت و آرشیو کنید!

این مورد را در بالا هم گفتیمو. اکنون تاکید می‌کنیم که حتما تصاویر موجود از سلفی‌ها و هر مورد شخصی را به کامپیتور 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!

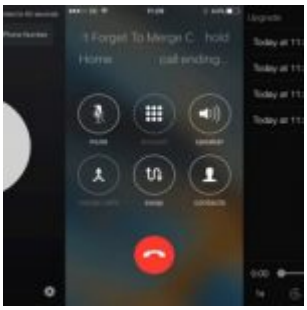
گوشی‌های کنونی همگی از سنسورها و چیپ‌های مختلفی بهره می‌برند، توجه کنید که روشن بودن آنها باعث مصرف باتری دستگاه شده و اجرای برنامه‌ها را با کند بودن همراه می‌کند! موارد اضافی را مثل gps، nfc بلوتوث و … را در مواقعی که کاری با انها ندارید خاموش نگاه دارید. برای اینکار کافی است نوار اعلانهای بالا صفحه 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. لطفا از نصب اپ‌های بیهوده و بی نام 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 بی مورد و نمایش تبلیغات در صفحه گوشی خواهند شد.

منبع: بیتوته

ضبط مکالمات تلفنی



چه در حال مصاحبه باشید یا می خواهید یک مکالمه‌ی خدمات مشتریان بد را برای آینده ضبط کنید، گزینه‌های شما این‌ها هستند.

دلایل زیادی برای ضبط مکالمات وجود دارد، مثل‌اینکه شما با یک نفر مصاحبه‌ی شغلی می‌کنید یا در حال بازاریابی هستید. سؤال اصلی این است که چگونه مکالمات خود را ضبط کنیم، ابزارهای زیادی برای این کار وجود دارد، اما قبل از اینکه از هرکدام استفاده کنید مطمئن شوید کار شما قانونی است.

ابزارهای ضبط مکالمات

اگر فرض کنیم شما مشکل قانونی ندارید چگونه باید یک مکالمه‌ی تلفنی را ضبط کنیم؟

بدیهی‌ترین روش این است: تماس را فارغ از نوع تلفنی که استفاده می‌کنید روی حالت بلندگو قرار دهید، سپس با یک دستگاه ثانویه تماس را ضبط کنید. این دستگاه ثانویه می‌تواند از یک میکروفون هدستی دیجیتال و وبکم پی سی (صدا هم ضبط می‌کند) گرفته تا یک اسمارت فون با هر اپ ضبط صدایی باشد.

ضعف این روش این است که بلندگو تمام صداهای محیط را نیز بلند می‌کند. اگر شما هنگام صحبت کردن تایپ کنید(مثل هنگام مصاحبه)، چیک چیک کیبورد شما ممکن است صدای زائدی روی صدای ضبط‌شده‌ی شما باشد.

Google Voice گزینه‌ی بهتری است. این سرویس ضبط صدا را به طرز عجیبی آسان می‌کند: تنها کافی است هنگام مکالمه ۴ را فشار دهید تا ضبط شروع شود، سپس دوباره ۴ را فشار دهید تا ضبط متوقف شود. وقتی‌که کارتان تمام شد، شما یک فایل mp3 خواهید داشت که می‌توانید آنلاین گوش کنید یا آن را دانلود کنید. فقط به یاد داشته باشید که این برنامه ابتدا شروع ضبط را اعلام می‌کند، پس نمی‌توانید این کار را در خفا انجام دهید.

همچنین این سرویس فقط هنگامی‌که با شما تماس گرفته می‌شود کار می‌کند، اگر شما باکسی تماس بگیرید، مثل تماس با خدمات مشتریان، این برنامه کمکی نخواهد کرد.(راه حرفه‌ای: می‌توانید از GetHuman استفاده کنید تا یک تماس از خدمات مشتریان به شماره Google Voice گرفته شود تا تماس‌های بیرونی را هم ضبط کنید)

اگر شما بایستی قادر به ضبط تماس‌های بیرونی یا کنفرانسی باشید، Recordator را امتحان کنید. این برنامه بی پلتفرم(Platform-agnostic) است یعنی با تلفن ثابت، تلفن همراه و غیره کار می‌کند. این بدین خاطر است که بر تماس سه مسیره تکیه می‌کند. به طرز مؤثری مکالمه‌ی شمارا به یک سرویس ضبط وصل می‌کند. بااین‌وجود این سرویس مجانی نیست. هم‌زمان با ضبط هزینه برای شما لحاظ می‌شود و چیزی حدود ۰٫۱ دلار بر دقیقه است.

شما همچنین می‌توانید از گزینه‌های اپلیکیشنی استفاده کنید. به‌عنوان‌مثال Call Recorder – ACR می‌تواند به‌سادگی تماس‌های ورودی و خروجی را ضبط کند اما حواستان باشد ابتدا امتحانش کنید چون تمام گوشی‌ها از ضبط کردن پشتیبانی نمی‌کنند.

کاربران آیفون می‌توانند چیزی مثل Call Recorder Free را امتحان کنند که شباهت آن با Recordator این است که بر تماس سه مسیره برای اتصال شما به یک خط ضبط کننده تکیه می‌کند. اما به یاد داشته باشید باوجوداینکه نسخه‌ی مجانی تمام مکالمه‌ی شمارا ضبط می‌کند، فقط ۶۰ ثانیه‌ی اول بازپخش می‌شود مگر اینکه شما نسخه‌ی Pro را خریداری کنید($۹٫۹۹). همچنین TapeACall وجود دارد که $۷٫۹۹ سالانه

هزینه دارد و هم تماس‌های ورودی و هم خروجی را ضبط می‌کند پرداخت این مبلغ، ضبط بدون محدودیت را در اختیار شما می‌گذارد و برای هر دقیقه مبلغی وجود ندارد.

اما گزینه‌ی دیگری نیز هست: یک اپ Voice-over-IP که از ضبط تماس پشتیبانی کند، به‌عنوان‌مثال WePhone به شما امکان تماس راه دور و بین‌المللی را می‌دهد و برای ضبط و توقف ضبط مکالمه کافی است یک کلید را فشار دهید.

کاربران همچنین از اپ هایی مثل RecordiaPro، FireRTCT و Yallo یادکرده‌اند.

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 کافیست 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 Contacts، Mail و Calendars را انتخاب کنید، پس از ورود به این بخش بر روی add کلیک کرده و 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 رابا موبایل همگام کند باید حواستان 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 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 More ، Import 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، اپلیکشین 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 ببنید.

منبع:بیتوته