

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

مراقب این بدافزار تلگرامی باشید.



بدافزار با عنوان سرویس تماس صوتی و تصویری تلگرام در حال انتشار است، این بدافزار سبب می شود تمام گروههای فرد پاک شده و این پیام برای همه افراد لیست دوستان فرد ارسال می شود.

به گزارش جام جم آنلاین، توصیه می شود که کاربران تلگرام برای نصب و به روز رسانی این برنامه به فروشگاه های معتبر اپلیکیشن مراجعه کنند.

سرویس تماس صوتی و تصویری تلگرام منتشر شد.
برای دانلود به لینک زیر مراجعه کنید:

<http://telgram.news/index.html>

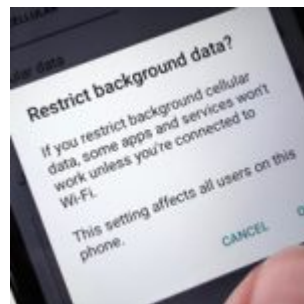
Telegram



Video & Voice Call



اعمال محدودیت دسترسی برنامه‌های اندرویدی به اینترنت

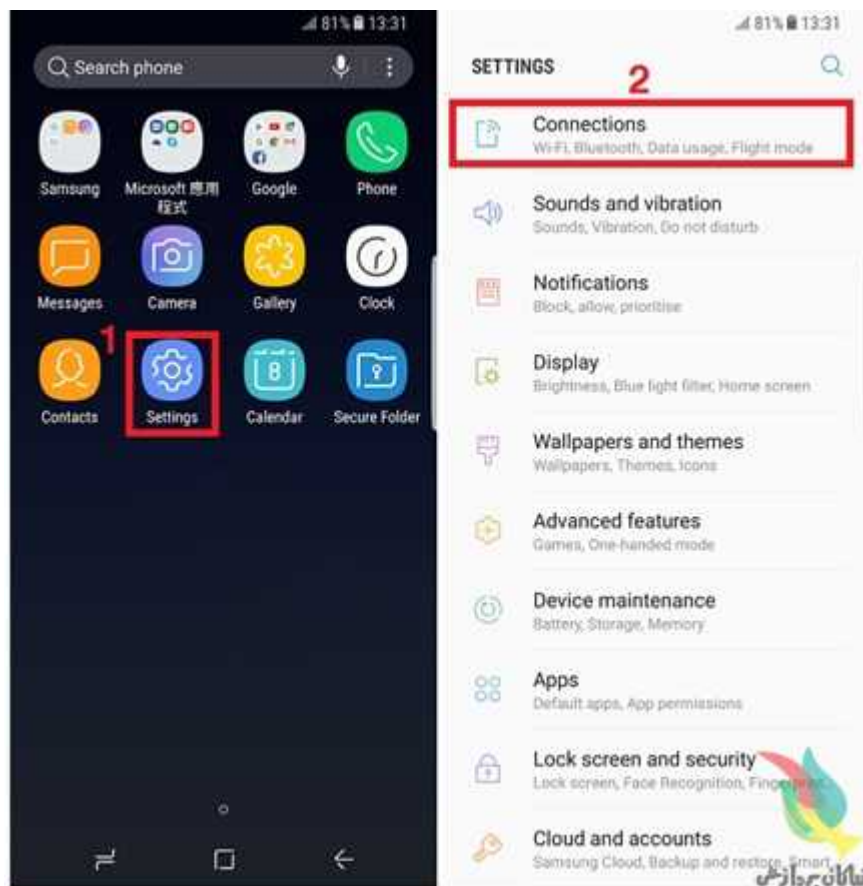


تاکنون چند مرتبه این اتفاق ناخوشایند را تجربه کرده‌اید که برنامه‌های کاربردی گوشی اندرویدی شما بدون اطلاع به اینترنت متصل شده‌اند، داده‌هایی را دریافت کرده یا ارسال کرده‌اند؟ ما در این مقاله راهکار جالبی را به شما معرفی می‌کنیم تا ضمن صرفه‌جویی در پهنای باند بتوانید مانع از آن شوید تا برنامه‌ها در پس‌زمینه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

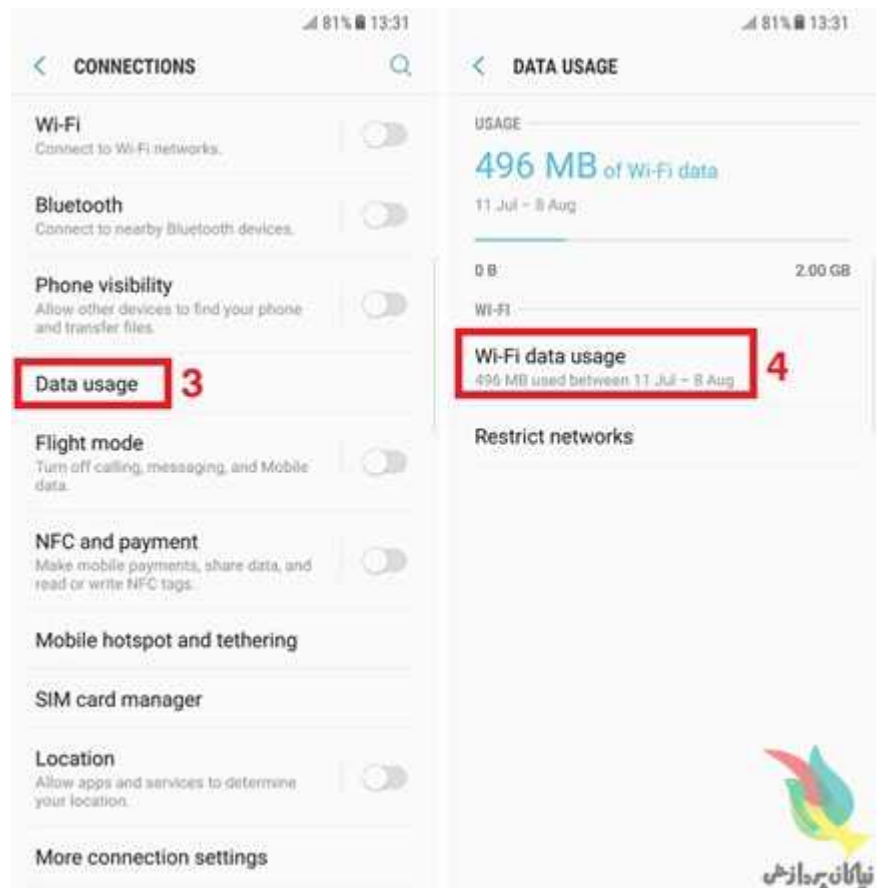
کاربران اندرویدی یک راهکار ساده اما ایده‌آل در اختیار دارند که به آن‌ها اجازه می‌دهد دسترسی برنامه‌های خاص به اینترنت را مسدود کنند. با توجه به این‌که امروزه برنامه‌های زیادی روی دستگاه اندرویدی شما نصب می‌شوند، جای تعجب نیست که بسیاری از این برنامه‌ها بدون اطلاع شما به اینترنت متصل شوند. این اتفاق از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

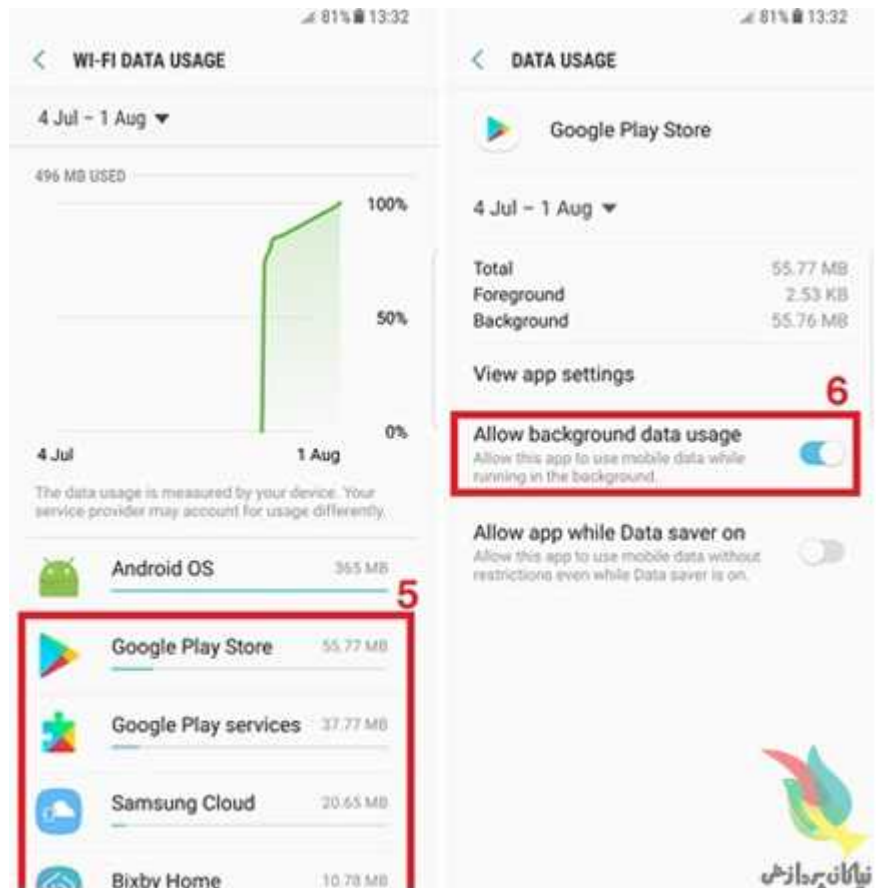
گام اول، در گوشی اندرویدی (سامسونگ) به بخش Settings بروید. اکنون گزینه Connections را انتخاب کنید.



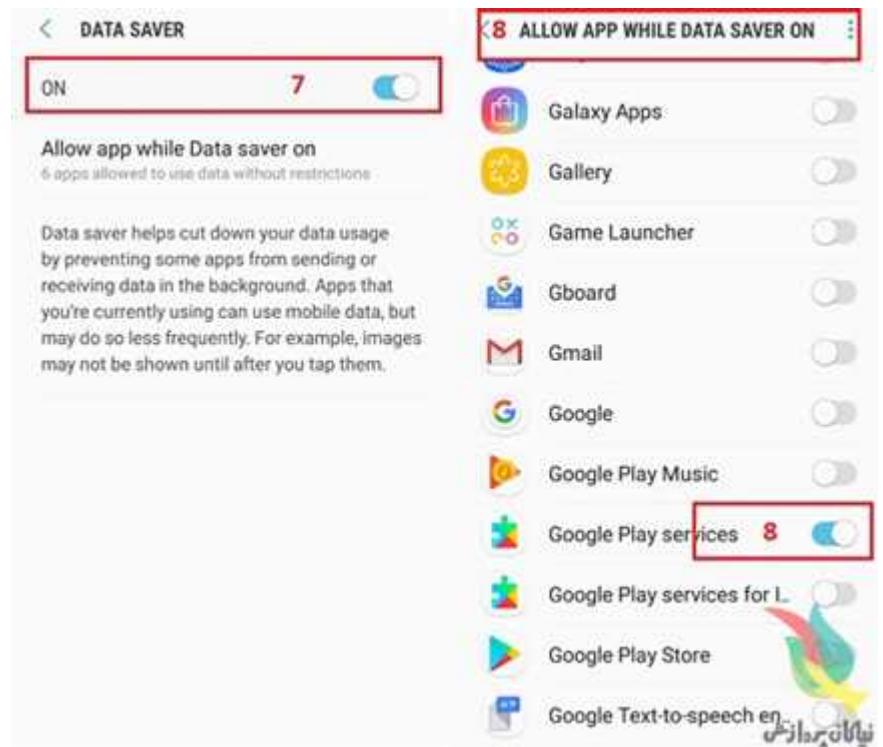
گام دوم، اکنون گزینه Data usage را انتخاب کرده و در ادامه گزینه Wi-Fi را انتخاب کنید.



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

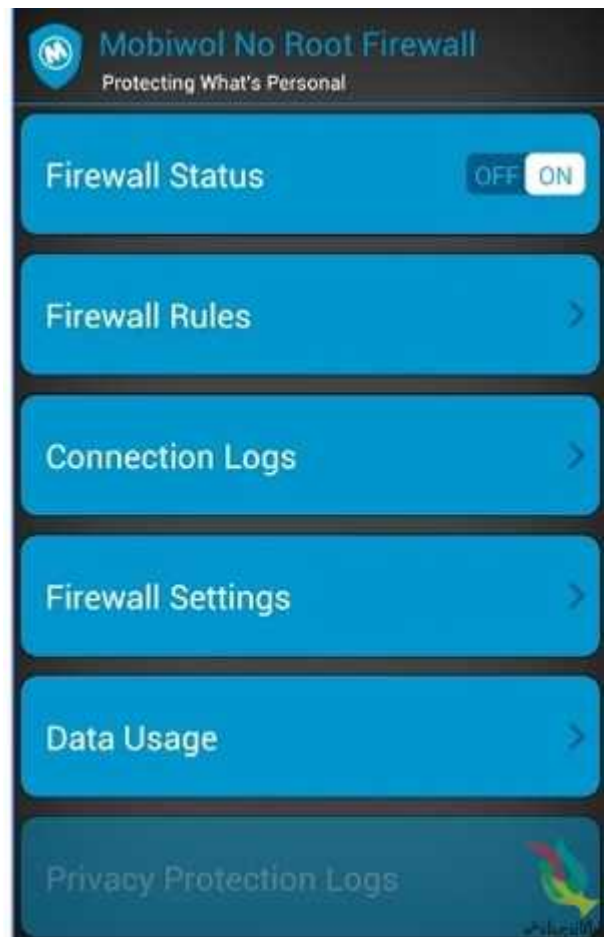
گام اول، ابتدا برنامه Mobiwol را از فروشگاه گوگل پلی دانلود کرده و روی گوشی خود نصب کنید

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

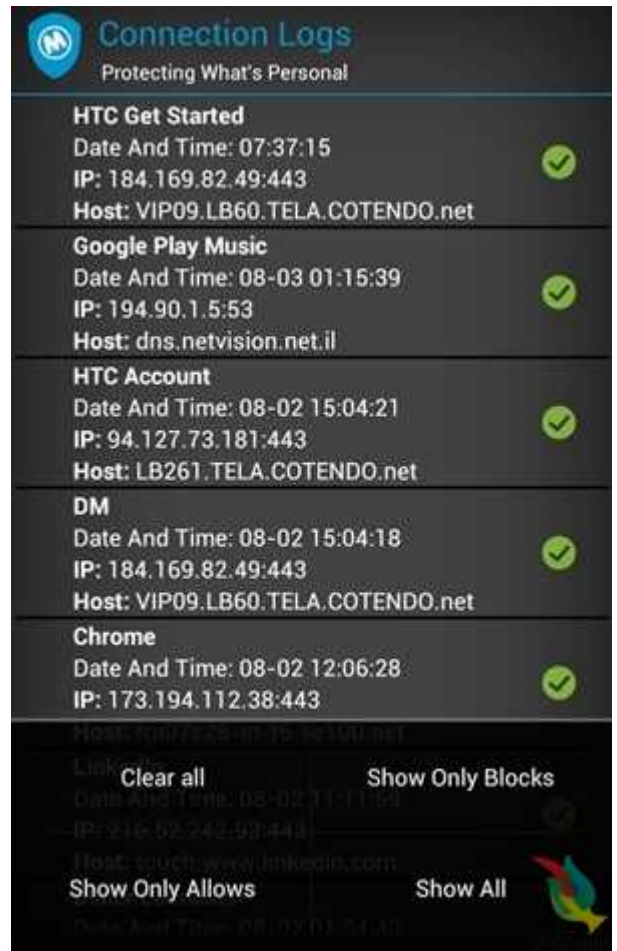
گام سوم، اکنون فهرستی از برنامه‌های کاربردی که روی گوشی شما نصب شده‌اند را مشاهده می‌کنید. در مقابل هر کدام از این برنامه‌ها دو گزینه وجود دارد. یکی از این گزینه‌ها اجازه دسترسی به وای‌فای و دیگری اجازه دسترسی به اینترنت موبایلی در پس‌زمینه دستگاه را به برنامه کاربردی تخصیص می‌دهند.



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.

آیا می‌توان به گوگل ترنسلیت اعتماد کرد؟



بسیاری از دانشجویان به خصوص در مقطع کارشناسی ارشد و دکترا برای انجام پروژه‌های کلاسی، پایان‌نامه و تحقیق و مطالعه منابع درسی با

ترجمه تخصصی سر و کار دارند.

شاید یکی از اولین راه‌هایی که برای ترجمه مقاله و متون انگلیسی به ذهن خطور کند، استفاده از گوگل ترنسلیت یا همان ترجمه ماشینی گوگل است. اما سوال این است که آیا واقعا این ترجمه ماشینی قابل اعتماد است و ترجمه متن را درست و دقیق انجام می‌دهد؟

در واقع باید گفت شاید برای ترجمه یک لغت یا یک جمله یا اصطلاح تا حدی بتوان به این مدل ترجمه آنلاین اعتماد کرد، اما اگر یک پاراگراف را با استفاده از آن ترجمه کنید خواهید دید که متن ترجمه شده تقریبا بی معنی و پر از کلمات بی ربط به موضوع است. حتی در مورد معنی لغات نیز بهتر است به جای گوگل ترنسلیت از یک دیکشنری انگلیسی به فارسی مثل آکسفورد استفاده کنید، زیرا هر کلمه می‌تواند معانی مختلفی داشته باشد و بسته به موقعیت قرارگیری در جمله ترجمه می‌شود که گاهی ترجمه ماشینی شما را به اشتباه می‌اندازد.



راه دیگری که بعضی از دانشجویان کمی مسلط به زبان انگلیسی انتخاب می‌کنند این است که خودشان ترجمه مقاله تخصصی را انجام دهند. اما وقتی شروع به کار ترجمه می‌کنند، می‌بینند که این کار آن‌قدرها هم به نظر می‌آید آسان نیست. تسلط به زبان انگلیسی با مهارت و دانش ترجمه انگلیسی بسیار متفاوت است. زبان انگلیسی پر از اصطلاحات و کنایه‌های ناآشنا و عجیب و غریب است و اگر معنای اصطلاح را ندانید ممکن است به اشتباه معنی ظاهری و تحت الفظی آن را استفاده کنید. علاوه بر این، اگر مترجم حرفه‌ای نباشید این کار برای شما بسیار وقت گیر است و زمانی را که می‌توانید برای مطالعه و تحقیق بیشتر اختصاص دهید باید برای ترجمه صرف کنید و در آخر هم ممکن است

نتیجه کار خیلی رضایت بخش نباشد.



پیشنهاد ما به شما استفاده از سامانه ترجمه آنلاین فارسیز است. با توجه به هزینه بالای ترجمه شاید برای بسیاری از دانشجویان مراجعه به دارالترجمه‌ها مقرون به صرفه نباشد. برای حل این مشکل فارسیز، ترجمه دانشجویی با کیفیت برنزی و نقره‌ای که اقتصادی و به صرفه است را پیشنهاد می‌کند. وقتی **ترجمه مقاله** و متون انگلیسی را به فارسیز می‌سپارید از کیفیت ترجمه مطمئن باشید زیرا ما با برگزاری آزمون‌های مترجمی و نظارت کارشناسان در سطوح مختلف، گروهی از بهترین مترجمان را گرد هم آورده‌ایم. اگر فرصت مراجعه حضوری به مراکز خدمات ترجمه را ندارید، باید خاطرنشان کنیم که روال کار ما از لحظه ثبت سفارش تا تحویل متن ترجمه شده و تایپ شده کاملاً آنلاین و از طریق سامانه می‌باشد. بنابراین تنها با چند کلیک می‌توانید سفارش ترجمه را ثبت کنید، هزینه را آنلاین پرداخت کنید و ترجمه را آنلاین دریافت کنید.

برای مراجعه به وب سایت سامانه ترجمه آنلاین فارسیز کلیک کنید.

منبع: بیتوته

امن‌ترین پیام‌رسان‌های دنیا کدامند؟



۱. واتس اپ (whatsapp)

اپلیکیشن پیام‌رسان واتس اپ در سال ۲۰۱۶ میلادی، محبوب‌ترین و پرکاربردترین پیام‌رسان توسط کاربران در سراسر جهان شناخته شد. این پیام‌رسان همچنین با توجه به اینکه از سیستم رمزنگاری پیشرفته end-to-end encryption بهره می‌برد، از ضریب امنیتی بالایی برخوردار است بدین گونه که مکالمات و اطلاعات مبادله شده میان کاربران و مخاطبان به صورت کامل محافظت شده بوده و این طور که گزارش‌های منتشر شده عنوان می‌کنند، مکالمات و اطلاعات شخصی و خصوصی آنها از سوی نهادهای دیگر قابل رصد و ردگیری نخواهد بود.

شرکت فیس‌بوک با در اختیار گرفتن و تصاحب شرکت واتس‌اپ در سال ۲۰۱۴، ۱۹ میلیارد دلار کسب کرد و از آن زمان تاکنون نیز با معرفی و افزودن قابلیت‌های جدید بدنبال جذب و حفظ طرفداران این پیام‌رسان محبوب بوده است.

۲. سیگنال (Signal)

این پیام‌رسان که در سال ۲۰۱۴ میلادی آغاز به کار کرد، توانست در این مدت

زمان کوتاه فعالیتش، به ضریب امنیتی بالایی دست یابد، هرچند که محبوبیت و آوازه آن چندان به اندازه سایر اپلیکیشن‌های پیام رسان معروف در جهان نشده است، اما بسیاری از متخصصان امنیت سایبری استفاده از آن را به عنوان یک پیام‌رسان امن به کاربران پیشنهاد می‌دهند. شیوه رمزنگاری این پیام رسان از واتس‌آپ تبعیت کرده و هیچ اطلاعاتی در سرویس‌ها و سرورهای اپلیکیشن سیگنال ذخیره نمی‌شود.

۳. جی دیتا چت (G data secure chat)

اپلیکیشن پیام‌رسان جی دیتا چت که به تازگی عرضه شده و به صورت رایگان در دسترس عموم کاربران قرار گرفته است، نیز چندان از محبوبیت سایر اپلیکیشن‌های معروف و همچنین تعداد دفعات دانلود زیادی برخوردار نشده است.

۴. تلگرام (telegram)

اپلیکیشن پیام‌رسان تلگرام هم که در دو سال اخیر از محبوبیت و استقبال بی نظیری از سوی کاربران بهره‌مند شده است، از سرعت و امنیت بالایی برخوردار است و علاوه بر پروتکل‌های رمزنگاری پیشرفته از قابلیت دیگری همچون مکالمه محرمانه (secret chat) برخوردار است.

۵. سیراس (Ceerus)

یکی دیگر از سرویس‌های پیام رسان اندرویدی، سیراس (Ceerus) نام دارد که توسط یک استارت‌آپ انگلیسی مجهز به سیستم‌های SQR معرفی و عرضه شده است. این اپلیکیشن که به منظور حفاظت از اطلاعات خصوصی و شخصی کاربران، شرکت‌ها و سازمان‌های مختلف طراحی و عرضه شد، از کاربران یک حساب کاربری کامل تهیه می‌کند و از سیستم رمزنگاری پیشرفته بهره می‌برد.

۶. پرایویت (Pryvate)

این سرویس پیام‌رسان نیز که در سال ۲۰۱۵ میلادی طراحی شد و در دسترس عموم کاربران قرار گرفت، از تماس صوتی و ویدیویی و مکالمات رمزنگاری شده بهره می‌برد و به کاربران در سیستم‌های عامل مختلف، خدمات ارسال پیام را ارائه می‌دهد. این پیام رسان توسط تجار و شرکت‌های تجاری از استقبال بی نظیری مواجه شده است.

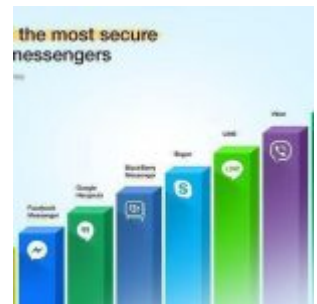
۷. فیس بوک مسنجر

پیام رسان فیس بوک مسنجر نیز از سیستم رمزنگاری پیشرفته end-to-end encryption و همچنین مکالمات محرمانه استفاده می‌کند و طبق گزارش‌های

منتشر شده، کاربران فیس بوکی از این پیام رسان استقبال زیادی کرده اند.

منبع: بیتوته

ده مسنجر معتبر و امن دنیا !!!



ایران پرچم دار انقلاب صنعتی چهارم



1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16
17	18	19	20
21	22	23	24
25	26	27	28
29	30	31	32
33	34	35	36
37	38	39	40
41	42	43	44
45	46	47	48
49	50	51	52
53	54	55	56
57	58	59	60
61	62	63	64
65	66	67	68
69	70	71	72
73	74	75	76
77	78	79	80
81	82	83	84
85	86	87	88
89	90	91	92
93	94	95	96
97	98	99	100

وزیر ارتباطات با انتشار آمار
کسبوکارهای اینترنتی به تفکیک
استانی در اینستاگرامش نوشت:
با رفع موانع، ایران پرچم دار
انقلاب صنعتی چهارم در منطقه
خواهد بود.



رتبه در بهمن ۹۵	رتبه در مرداد ۹۶	نام شهر	تعداد در مرداد ۹۶	تعداد در بهمن ۹۵
۱	۱	تهران	۱۳۴۹۲	۱۰۶۵۷
۲	۲	خراسان رضوی	۲۲۷۲	۱۸۰۹
۳	۳	اصفهان	۲۲۲۴	۱۷۸۰
۴	۴	فارس	۱۵۲۹	۱۱۸۱
۵	۵	آذربایجان شرقی	۱۰۶۰	۸۳۹
۶	۶	البرز	۹۳۹	۷۵۰
۷	۷	مازندران	۷۴۵	۵۷۹
۸	۸	گیلان	۶۶۷	۵۴۹
۹	۹	خوزستان	۶۱۵	۴۸۷
۱۰	۱۰	قم	۵۷۵	۴۷۹
۱۱	۱۱	آذربایجان غربی	۴۹۵	۴۱۰
۱۲	۱۲	یزد	۴۸۶	۳۸۴
۱۳	۱۳	هرمزگان	۴۱۹	۳۲۳
۱۴	۱۴	کرمان	۳۷۹	۳۰۰
۱۶	۱۵	گلستان	۳۰۱	۲۳۲
۱۵	۱۶	قزوین	۲۹۰	۲۴۲
۱۸	۱۷	مرکزی	۲۷۵	۲۱۵
۱۷	۱۸	بوشهر	۲۵۵	۲۱۷
۱۹	۱۹	اردبیل	۲۳۷	۱۹۹
۲۱	۲۰	کرمانشاه	۲۳۷	۱۸۶
۲۰	۲۱	کردستان	۲۳۲	۱۸۹
۲۲	۲۲	همدان	۲۲۵	۱۷۴
۲۴	۲۳	زنجان	۲۱۵	۱۵۸
۲۳	۲۴	سمنان	۲۱۱	۱۶۸
۲۵	۲۵	خراسان جنوبی	۱۷۸	۱۴۲
۲۶	۲۶	لرستان	۱۳۲	۹۹
۲۷	۲۷	چهارمحال و بختیاری	۱۱۶	۸۷
۲۸	۲۸	خراسان شمالی	۱۱۳	۸۳
۲۹	۲۹	سیستان و بلوچستان	۱۰۲	۷۸
۳۰	۳۰	کهگیلویه و بویراحمد	۵۳	۴۴
۳۱	۳۱	ایلام	۵۱	۴۴

مقایسه رتبه تعداد کسب و کارهای استان
ها نسبت به رتبه آنها در بهمن ۹۵

رتبه برابر رتبه بالاتر رتبه پایین تر

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.



هزینه ی عنوان شده توسط محافظان اندروید در برابر برنامه های 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.

مراقب اطلاعاتتان باشید!



با توجه به حملات سایبری هکرها در چند روز اخیر به سایت های دولتی و شرکت های بزرگ دنیا و حجم خسارات وارد شده به اطلاعات سازمان ها لازم است نکات زیر را رعایت نموده و راهکارهای پیشنهاد شده را با درجه اهمیت بالا انجام دهید:

حملات از نوع باج گیرها می باشند این نرم افزارها بدلیل ماهیت کاری که انجام می دهند از دید آنتی ویروس ها پنهان هستند و اطلاعات اسنادی (Word, Excel, Access, Powerpoint, PDF, E.Mail, SQL, Text) را رمزنگاری می کنند. فایل های رمزنگاری شده صرفا در قبال پرداخت مبالغ زیاد قابل استفاده می باشند و لازم به توضیح است که تاکنون هیچ روشی برای بازگشت و یا بازیابی داده های رمزنگاری شده وجود ندارد.



لازم است نکات پیشگیرانه زیر را مد نظر قرار دهید تا در دام این حملات گیر نیافتید:

۱ - از اطلاعات مهم کاری خود بر روی لوح فشرده CD یا DVD در زمان های متعدد پشتیبان تهیه کنید. توجه داشته باشید که لوح فشرده بعد از عمل رایت (Write) امکان آلوده شدن ندارد.

۲ - تحت هیچ شرایطی ایمیل های مشکوک را باز نکنید. ایمیل های مشکوک عموماً با پیشنهادهای مهیجی از قبیل برنده شدن در یک مسابقه یا ... می باشد. توجه داشته باشید اینگونه ایمیل ها عموماً از آدرس دوستان شما که هک شده اند برای شما ارسال می شود.

۳ - بر روی لینک های خبرهای مهیج مخصوصاً در این بازه زمانی که با اخبار انتخابات نیز همراه می شود کلیک نکنید. برای مطالعه اخبار به سایت های معتبر خبرگزاری مراجعه کنید و از باز کردن لینک اخبار یا تصاویر و ... در نرم افزارهای شبکه های اجتماعی خودداری کنید.

۴ - به هیچ عنوان از نرم افزارهای شبکه های اجتماعی بر روی سیستم های رایانه ای استفاده نکنید. سعی کنید از نسخه های موبایلی آن شبکه ها استفاده کنید.

۵ - آنتی ویروس تان را بروز نگه دارید و از آنتی ویروس های کرک شده استفاده نکنید.

۶ - اگر دستگاه های ذخیره ساز مانند فلش یا هارد اکسترنال به سیستم خود متصل می کنید قبل از بازکردن آن ها را با آنتی ویروس اسکن کنید.

۷ - در صورتی که به باج گیر آلوده شدید(فایل های اسنادی شما به درستی باز نمی شوند و با پیامی مبنی بر رمز شدن اطلاعات مواجه شدید) بلافاصله کابل شبکه را از کامپیوتر خود جدا نمایید.

۸ - تاکید می شود حتما از داده های حساس خود بر روی لوح های CD و یا DVD فایل پشتیبان تهیه نمایید. همچنین می توانید با بهره گیری از نرم افزارهای فشرده سازی چون Winrar فایل های خود را فشرده نموده و ذخیره کنید.

تصویری گویا از علل حملات مهاجمان به گوشی ها





چرا گوشی های تلفن همراه هدف مجرمان سایبری قرار می گیرند؟

✓ تلفن همراه شما، همه چیز را در مورد شما می داند.

اطلاعاتی نظیر: تصاویر خصوصی، اطلاعات شخصی و حساب های شبکه های اجتماعی، اطلاعات حساب بانکی و ... از جمله اهداف مجرمان سایبری اند.



✓ تلفن های همراه می دانند شما کجا هستید و کجا کار می کنید.

زمانی که از GPS گوشی خود استفاده می کنید امکان ردیابی موقعیت خود را فراهم کرده اید.



✓ تلفن همراه شما، مسیری به سمت کیف پولتان است.

استفاده از نرم افزار های بانکی در کنار مزایای خود می تواند به یکی از اهداف مجرمان سایبری تبدیل شود.



✓ تلفن های همراه به وسیله ای در شرکت ها و سازمان ها تبدیل شده است.

استفاده از تلفن های همراه در محل کار شرایطی را ایجاد کرده تا این ابزار به عنوان دروازه ای برای سرقت اطلاعات حساس سازمان ها محسوب شود.



نیانک پردازش