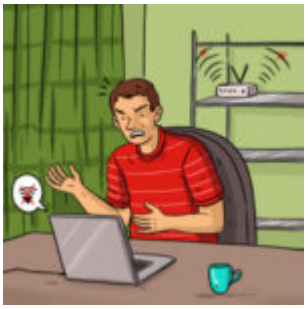
۸ موردی که می توانند وای فای شما را ضعیف کند.



گاهی اوقات ، این مشکل در تنظیمات روتر یا سرویس ضعیف ارائه شده توسط شرکت ارائه دهنده سرچشمه می گیرد. اما بیشتر اوقات ، اتصال WiFi بد به دلیل وجود اشیا یا مبلمان خاصی که در خانه داریم بسیار نزدیک به روتر یا رایانه های ما ایجاد می شود.

در این مطلب به شما می گوییم دشمنان اصلی WiFi کدام آیتم هستند. نکات مفیدی را در انتهای مقاله خواهید یافت که می توانید از آنها برای جلوگیری از آنتن دهی ضعیف استفاده کنید ، آنها را از دست ندهید!

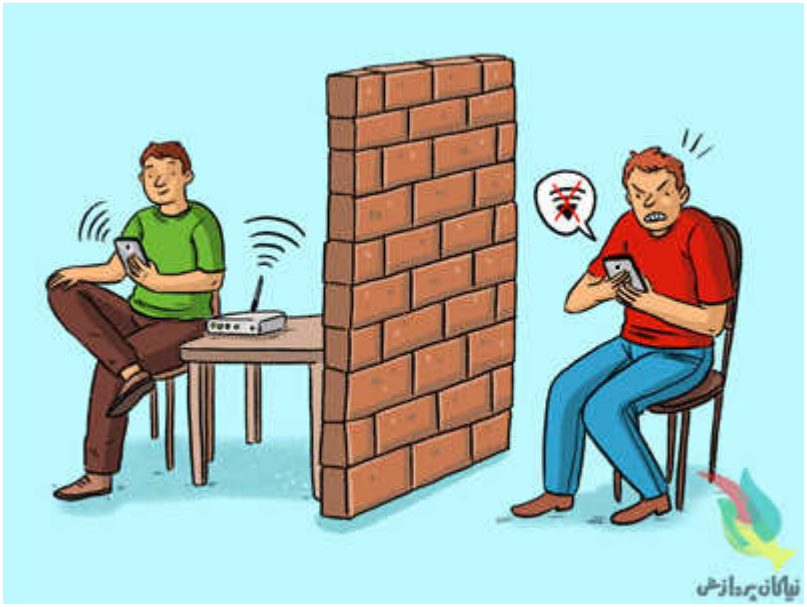
۱-سطوح و مبلمان فلزی



فلز رسانا است ، به این معنی که الکتریسیته را جذب می کند. از آنجا که WiFi شما امواج الکترومغناطیسی را آزاد می کند ، هر سطح فلزی یا شیء در خانه شما از انتشار امواج جلوگیری می کند. اگر می

خواهید ارتباط اینترنت شما بدون مشکل کار کند، لازم است روتر را از فلز دور کنید.

۲-دیوارهای آجری و سنگی



برخی از انواع دیوارها سیگنال WiFi شما را متوقف می کنند. در بین رایج ترین مواد که مانع از اتصال قابل اعتماد می شود ، سنگ مرمر ، سیمان ، بتن ، گچ و آجر است. این مسئله توضیح می دهد که چرا در خانه های ۲ طبقه معمولاً افراد در یکی از طبقه ها اینترنت ضعیف را تجربه می کنند. برای رفع این مشکل ، روتر خود را در یک منطقه باز و به دور از دیوارها قرار دهید.

۳-آینه ها



ماده ای که به ما امکان می دهد بازتاب خود را در آینه مشاهده کنیم ، سیگنال منتشر شده توسط روتر را نیز منعکس می کند. این شیء به عنوان یک سپر عمل می کند و باعث می شود اتصال به اینترنت مشکل شود. هنگامی که به روتر نزدیک باشد ، می تواند باعث شود استحکام سیگنال کندتر و ناپایدار باشد.

۴-یخچال و ماشین لباسشویی



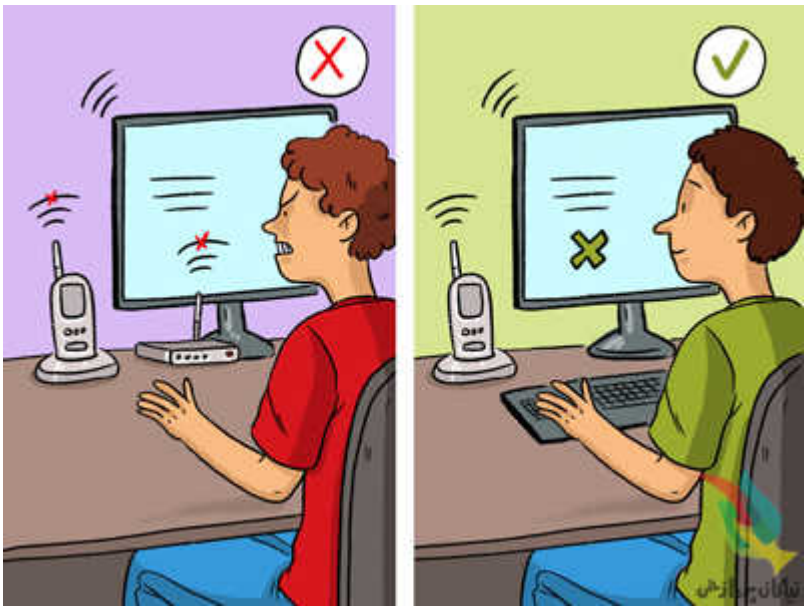
به عنوان یک قاعده کلی ، وسایل برقی که دارای لوله هایی هستند که آب را در گردش خود قرار می دهند با سیگنال WiFi خیلی دوستانه نیستند آب می تواند مقداری از انرژی را از امواج بی سیم حفظ کند ، که بر کیفیت اتصال به اینترنت تأثیر منفی می گذارد.

۵-چراغ های کریسمس



چراغ های رنگارنگ کریسمس همچنین می تواند دلیل وجود سیگنال ضعیف WiFi در خانه باشد. آنها دارای تراشه های درخشان هستند که یک میدان مغناطیسی ایجاد می کنند که با امواج الکتریکی صادر شده توسط روتر شما در تعامل است. در ماه دسامبر ، سعی کنید روتر خود را از درخت کریسمس دور نگه دارید.

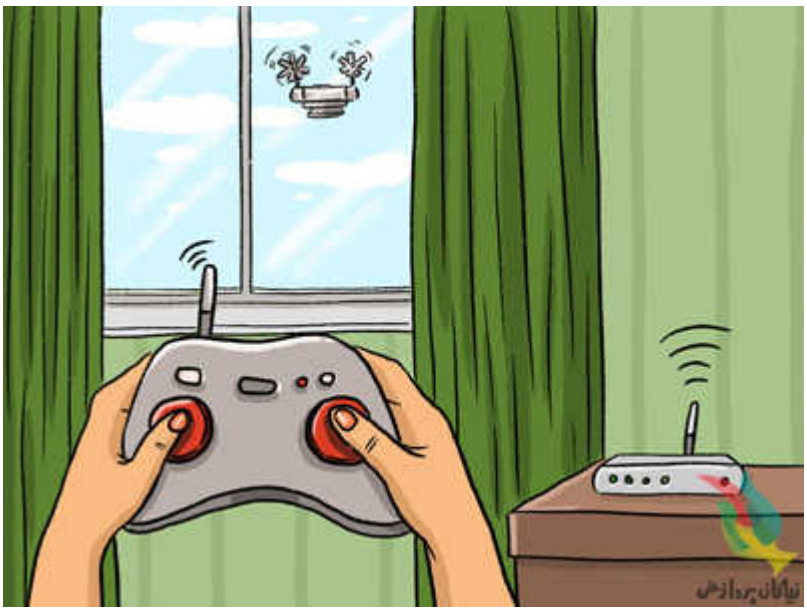
۶-مانیتور کودک



این مانیتورها یک تداخل ۲٫۴ گیگاهرتز تولید می کنند ، همان WiFi. وقتی ۲ یا چند دستگاه فرکانس یکسانی را منتقل می کنند، آنها از هوا برای ارسال اطلاعات به جای انتقال امواج استفاده می کنند، مانند مورد بی سیم. اگرچه مانیتورهای کودک معمولاً برای عملکرد صحیح به اتصال به یک شبکه نیاز دارند ، از قرار دادن آنها در

نزدیکی روتر خودداری کنید.

۷-هواپیماهای بدون سرنشین



هواپیماهای بدون سرنشین همچنین با سرعت ۲٫۴ گیگاهرتز کار می کنند ، اما همه مدل ها این اختلال را ایجاد نمی کنند. همه اینها به میزان توان مورد نیاز هر مدل بستگی دارد.

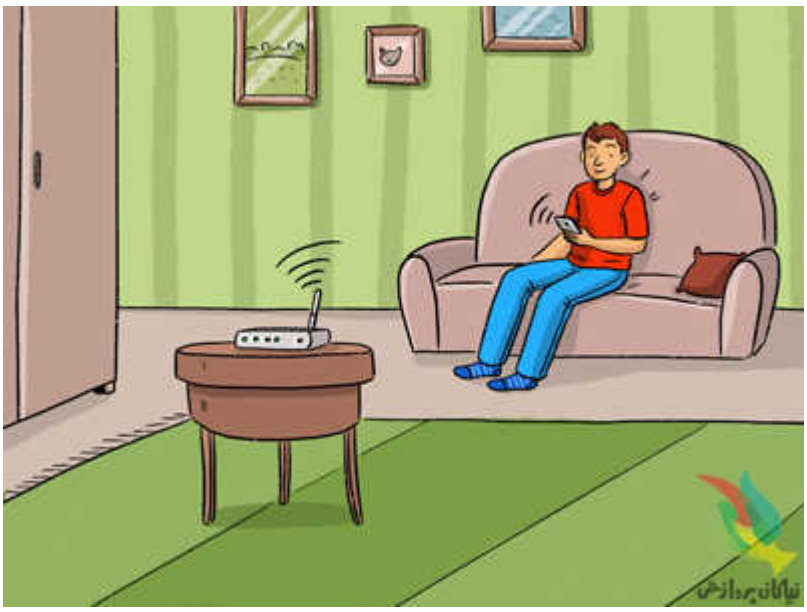
۸-مایکروویو



این دستگاه دیگری است که دارای طیف فرکانس مشابه دستگاه مورد استفاده WiFi است. اگر روتر خود را در نزدیکی مایکروویو قرار داده اید ، آن را به محلی بالاتر از سطح مایکروویو برسانید. این

به طور قابل ملاحظه ای اثر منفی مایکروویو را در اتصال کاهش می دهد.

پاداش: چگونه می توان اتصال WiFi خود را ارتقا داد؟



اقدامات مختلفی وجود دارد که می توانید برای بهبود ارتباط اینترنتی خود در خانه انجام دهید. اگر مرتباً با یک سیگنال بد روبرو هستید ، آنها را به خاطر بسپارید:

1. بر اساس موارد ذکر شده در بالا ، مکان مناسبی را برای قرار دادن روتر خود انتخاب کنید.
2. روتر خود را به روز کنید.
3. یک آنتن قدرتمند تر بدست آورید.

۴- وای فای خود را رمزگذاری کرده و با رمز قوی محافظت کنید، رمزی که به راحتی نمی توان حدس زد.

۵- یک تقویت کننده WiFi بخرید ، همچنین به عنوان توسعه دهنده WiFi شناخته می شود.

6. فقط از جدیدترین و مدرن ترین فن آوری های WiFi استفاده کنید.
7. پهنای باند هایی که در ۵ گیگاهرتز کار می کنند ، معمولاً ارتباطی بسیار سریعتر از سایرین ارائه می دهند ، زیرا این کانال کمتر از باند ۲٫۴ گیگاهرتزی شلوغ است.

۸- روتر را مجدداً تنظیم کنید ، این عمل حافظه آن را پاک می کند

و شما را قادر می سازد که به روزرسانی ها را نصب کنید.

منبع: بیتوته

چگونگی پاسخ دادن به پیام‌های واتس‌اپ بدون نیاز به آنلاین شدن



حتماً تا کنون برایتان پیش آمده که نخواهید به پیام یکی از دوستان خود در واتس‌اپ جواب دهید تا مبادا یک مکالمه طولانی آغاز شود. اگر به این شرایط تا حالا برخورد کرده‌اید، با ما همراه شوید تا چگونگی پاسخ دادن به یک پیام بدون نیاز به آنلاین شدن را آموزش ببینید.



پاسخ دادن از طریق اعلانات یا ساعت هوشمند

اگر پیام واتس‌اپ را دریافت کرده‌اید و اعلان آن در نوار اعلانات مشاهده

می‌شود، فقط کافی است روی گزینه ریپلای کردن (Reply) ضربه بزنید تا بتوانید به پیام جواب بدهید.
به علاوه، چنان‌چه یک ساعت هوشمند با سیستم عامل Android Wear دارید، می‌توانید بدون نیاز به آنلاین شدن، به پیام پاسخ دهید.
پاسخ دادن به صورت آفلاین

- همه اتصالات به اینترنت را قطع کنید
- واتس‌اپ را اجرا و گفتگویی که می‌خواهید به آن جواب دهید را باز کنید
- پاسخ خود را بنویسید
- واتس‌اپ را ببندید
- اینترنت را دوباره وصل کنید
- واتس‌اپ پیام شما را ارسال می‌کند بدون اینکه شما را آنلاین نشان دهد.

شناسایی مصرف‌کنندگان وب‌کم در ویندوز



وب‌کم یا همان دوربین‌های کوچکی که در لپ‌تاپ‌ها وجود دارد یا برخی کاربران به‌صورت مجزا تهیه کرده و در ارتباطات زنده تصویری از آن استفاده می‌کنند بسیار کاربردی است و لذت برقراری تماس با دوستان، آشنایان و فرزندان یا والدین را چند برابر می‌کند، اما در کنار این لذت فراوان، خطرات امنیتی زیادی نیز وجود دارد که به همین علت کارشناسان همواره به کاربرانی که از وب‌کم استفاده نمی‌کنند توصیه می‌کنند روی آن را بپوشانند.

اگر جزو کاربرانی هستید که از وب‌کم دستگاه خود استفاده می‌کنید ممکن است بخواهید در مواقعی که دوربین شما فعال و چراغ آن روشن می‌شود، برنامه‌ای را که موجب فعال‌سازی وب‌کم شده شناسایی کرده تا به این ترتیب با اطمینان و آرامش بیشتری از وب‌کم استفاده کنید و نگران هک شدن دستگاه خود نباشید. برای انجام این کار در ویندوز می‌توان از ترفندی که به کمک ابزار Process Explorer tool اجرا

می‌شود کمک گرفت. این ابزار توسط مایکروسافت منتشر شده و مشابه ابزار Task Manager ویندوز اما با امکانات بسیار بیشتر است.



پیش از هر چیز باید نام وب‌کم را در فهرست دستگاه‌های متصل به رایانه پیدا کنید. برای انجام این کار در ویندوزهای ۸ و ۱۰ می‌توانید روی منوی استارت کلیک راست ماوس را فشار دهید و گزینه Device Manager را انتخاب کنید. همچنین در ویندوز ۷ نیز کلیدهای Windows+R را فشار داده و پس از تایپ عبارت devmgmt.msc کلید اینتر را فشار دهید.

به بخش Imaging Devices مراجعه کرده و پس از انتخاب وب‌کم موجود در این بخش، روی آن کلیک راست کرده و گزینه Properties را انتخاب کنید.

روی تب Details کلیک کرده و از بخش Property گزینه Physical Device Object Name را انتخاب کنید.

روی مقدار به‌نمایش درآمده در بخش Value کلیک راست کرده و گزینه Copy را انتخاب کنید.

حالا باید ابزار Process Explorer را اجرا کنید. در صورتی‌که این ابزار را دریافت نکرده‌اید می‌توانید با مراجعه به لینک زیر آخرین نسخه از آن را دریافت و نصب کنید:

http://tiny.cc/click_proex

پس از اجرای این نرم‌افزار، کلیدهای Ctrl+F را فشار داده یا از منوی Find روی Find Handle or DLL کلیک کنید.

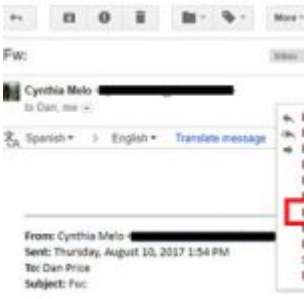
در بخش Handle or DLL Substring کلیک راست کرده و گزینه Paste را انتخاب کنید تا مقدار کپی شده در مرحله ۴ در این بخش وارد شود.

روی گزینه Search کلیک کنید تا نرم‌افزار Process Explorer عملیات جست‌وجوی برنامه‌هایی را که در حال استفاده از وب‌کم هستند، آغاز کند.

پس از مشاهده نتایج جست‌وجو در صورتی‌که نیازمند کسب اطلاعات بیشتر از هر برنامه باشید می‌توانید نام برنامه را در فهرست Processهای فعال پیدا کرده و با کلیک راست روی آن و انتخاب گزینه Properties اطلاعات بیشتری از برنامه موردنظر کسب کنید. همچنین در صورت مشکوک بودن هریک از برنامه‌ها می‌توانید با کلیک راست و انتخاب گزینه Kill Process آن برنامه را ببندید.

منبع: بیتوته

بلاک تمام ایمیل‌های مزاحم در جیمیل



یکی از مشکلاتی که همواره کاربران صندوق‌های پستی از جمله جیمیل را کلافه می‌کند ایمیل‌های مزاحم است. لزوما این ایمیل‌ها همیشه اسپم نیستند بلکه گاهی ممکن است تصمیم داشته باشید تا ایمیل‌های یکی از مخاطبان یا شرکت‌های مشهور را بلاک کنید. جیمیل برای رسیدن به‌این هدف راه‌کار بسیار ساده‌ای را در اختیار کاربران خود قرار داده است. با ماه همراه باشید.

اگر از کاربران اینترنت بخواهیم که لیستی از بدترین چیزهایی که با آن برخورد می‌کنند تهیه کنند ایمیل‌های ناخواسته در کنار پیام‌های توییتر و تبلیغات در صدر این فهرست جا دارند.

اما، مشکل فقط ایمیل‌های اسپم نیستند که حجم صندوق پستی را پر می‌کنند. در دنیای امروز که کاربران همیشه آنلاین هستند چقدر احتمال دارد که بتوانید برای یک مدت زمان مشخص صندوق خود را خالی نگه دارید؟

خوشبختانه، جیمیل فکر این قسمت را هم کرده و روش ساده‌ای برای بلاک کردن ایمیل‌ها از آدرس‌هایی که چندان علاقه‌ای به آن‌ها ندارید ارائه کرده است.

چگونه ایمیل‌ها را در جیمیل بلاک کنیم

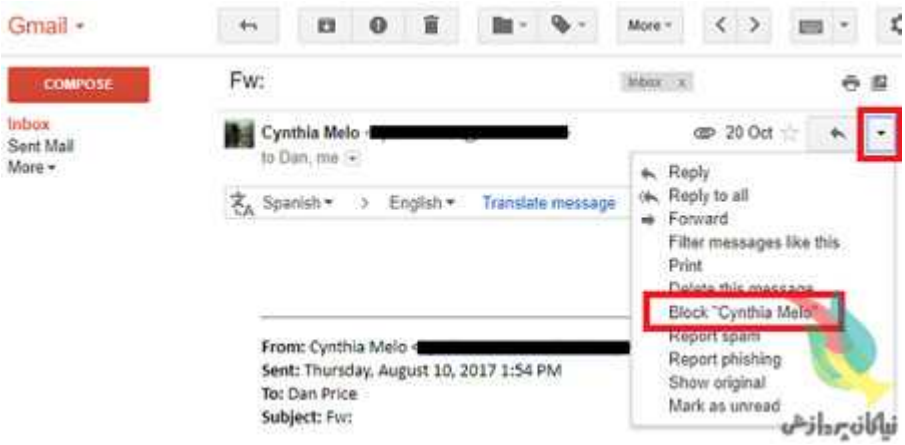
۱- در مرورگر خود به‌مسیر google.com/gmail بروید و با تایپ نام کاربری و گذرواژه وارد حساب کاربری‌تان شوید.

۲- ایمیل فرد، شرکت یا هر آدرس رندومی که قصد بلاک کردن آن‌را دارید پیدا کنید.

۳- ایمیل مربوطه را باز کنید.

۴- در همان خطی که نام و آدرس ارسال کننده وجود دارد روی فلش رو به‌پایین کلیک کنید.

۵- گزینه “Block “[Sender’s name/address را انتخاب کنید.



چگونه ایمیل‌ها را در جیمیل آنبلاک کنیم

اگر ایمیل یکی از مخاطبان خود را به‌طور تصادفی بلاک کرده‌اید، اصلا نگران

نباشید. به‌سادگی می‌توانید خودتان را از این مخمصه نجات دهید.

۱- جیمیل را باز کنید.

۲- روی آیکون چرخ دنده در سمت راست بالای صفحه کلیک کنید.

۳- وارد Settings شوید.

۴- روی تب Filters and Blocked Addresses در بالای صفحه کلیک کنید.

۵- به‌پایین صفحه بروید تا به‌گزینه The following email addresses are blocked. Messages from these addresses will appera in Spam برسید.

۶- آدرسی که قصد آنبلاک کردن آن‌را دارید هایلایت کنید.

۷- روی گزینه Unblock Selected Addresses کلیک کنید.

به‌همین سادگی می‌توانید ایمیل‌های مزاحم و کلافه کننده را بلاک کنید.

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 می دهد؟

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 کاملا 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

تصویری گویا از علل حملات مهاجمان به گوشی ها



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

✓ تلفن همراه شما، همه‌چیز را در مورد شما می‌داند.

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



✓ تلفن‌های همراه می‌دانند شما کجا هستید و کجا کار می‌کنید.

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.



✓ تلفن‌های همراه به وسیله‌ای در شرکت‌ها و سازمان‌ها تبدیل شده است.

استفاده از تلفن های همراه در محل کار شرایطی را ایجاد کرده تا این ابزار به‌عنوان دروازه‌ای برای سرقت اطلاعات حساس سازمان‌ها محسوب شود.



لوگوی گوگل را به دلخواه تغییر نام دهید.



گوگل یکی از پرکاربردترین مرورگرها در بین کاربران وب است، یکی از قابلیت‌های این مرورگر تغییر نام آن به دلخواه شماست.



لوگوی گوگل را همیشه با رنگ های مختلف دیده اید و گاه به مناسبت‌های گوناگون اشکالی متفاوت از لوگوی گوگل برای شما به نمایش گذاشته شده است، ممکن است عده ای تغییر نام لوگوی گوگل را یک قابلیت جذاب و مناسب برای این مرورگر بدانند که می تواند در کنار تمامی قابلیت های گوگل، این مرورگر را در بین کاربران محبوب تر از گذشته کند.

تغییر نام لوگوی با یک ترفند ساده قابل انجام است و شما می توانید پس از انجام مراحل زیر هر بار که گوگل را باز می کنید به جای نام google، عنوانی را که انتخاب کرده اید، ببینید.

برای شروع در مرورگر گوگل عنوان goglogo را تایپ کنید و اینتر را بزنید.

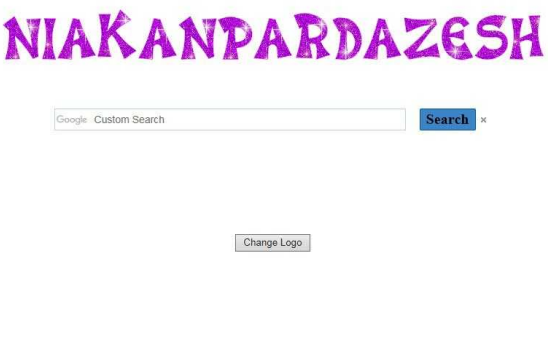
سپس سایتی که به شما معرفی شده است را باز کنید. در قسمت your name کلیک کنید.



نام دلخواه خود را تایپ کرده و اینتر را بزنید.



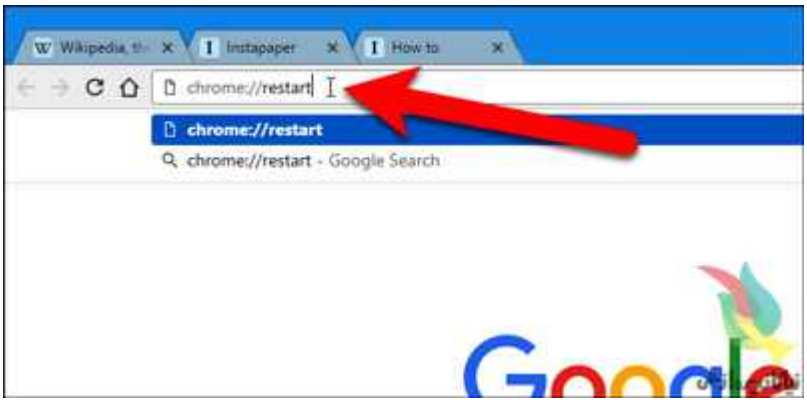
همانطور که در تصویر زیر مشاهده می کنید صفحه گوگل به نامی که شما انتخاب کرده اید تغییر پیدا کرده است.



ری‌استارت کروم با میانبر



در شرایط عادی مطمئنا نیازی به ری‌استارت کردن مرورگر (بستن و اجرای مجدد آن) وجود ندارد، اما گاهی ممکن است به هر دلیلی چاره‌ای جز این کار نداشته باشید.



رایج‌ترین روش برای ری‌استارت کردن مرورگر، استفاده از گزینه Close برای بستن آن و در ادامه اجرای مجدد با دوبار کلیک روی آیکون برنامه است. این روش مشکلی ندارد، اما همان‌طور که می‌دانید این صفحه به دوستداران ترفند اختصاص دارد و مرورگر کروم نیز مملو از قابلیت‌های پنهان است.

یکی از این قابلیت‌های پنهان مرورگر، دریافت فرمان‌های خاص با استفاده از نوار آدرس است. به‌عبارت دقیق‌تر مرورگر کروم قادر است مجموعه فرمان‌های مختلفی را با استفاده از نوار آدرس و تایپ عبارت chrome:// در اختیار شما قرار دهد که یکی از این فرمان‌ها نیز برای ری‌استارت کردن سریع مرورگر کاربرد دارد. این فرمان به‌شرح زیر است:

chrome://restart

اکنون که با این فرمان آشنا شدید می‌توانید به‌صورت یک ترفند برای ری‌استارت کردن سریع مرورگر از آن کمک بگیرید، ولی برای ساده‌تر شدن کار نیز یک ترفند دیگر را با این ترفند ترکیب می‌کنیم تا این فرمان را به فهرست سایت‌های دلخواه در مرورگر اضافه کنیم و بدون نیاز به تایپ فرمان، با یک کلیک روی آن، دستور ذکر شده را فراخوانی کنید. برای استفاده از این ترفند به این روش عمل کنید:

پیش از هر چیز مطمئن شوید نوار بوکمارک‌ها در مرورگر فعال است. برای اطمینان می‌توانید کلیدهای Ctrl+Shift+B را فشار دهید.

حالا به یک سایت دلخواه مراجعه کرده و آیکون آن را از سمت چپ نوار آدرس با روش کشیدن و رها کردن به داخل نوار بوکمارک انتقال دهید.

روی گزینه اضافه شده به نوار بوکمارک کلیک راست ماوس را فشار داده و گزینه Edit را انتخاب کنید.

در بخش Name عنوانی دلخواه همچون «ری‌استارت کروم» را وارد کنید.

در بخش URL نیز عبارت زیر را وارد کنید:

chrome://restart

با کلیک روی Save تغییرات را ذخیره کنید.

از حالا به بعد برای ری‌استارت سریع مرورگر کافی است روی گزینه ایجاد شده در نوار بوکمارک یک‌بار کلیک کنید.

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.

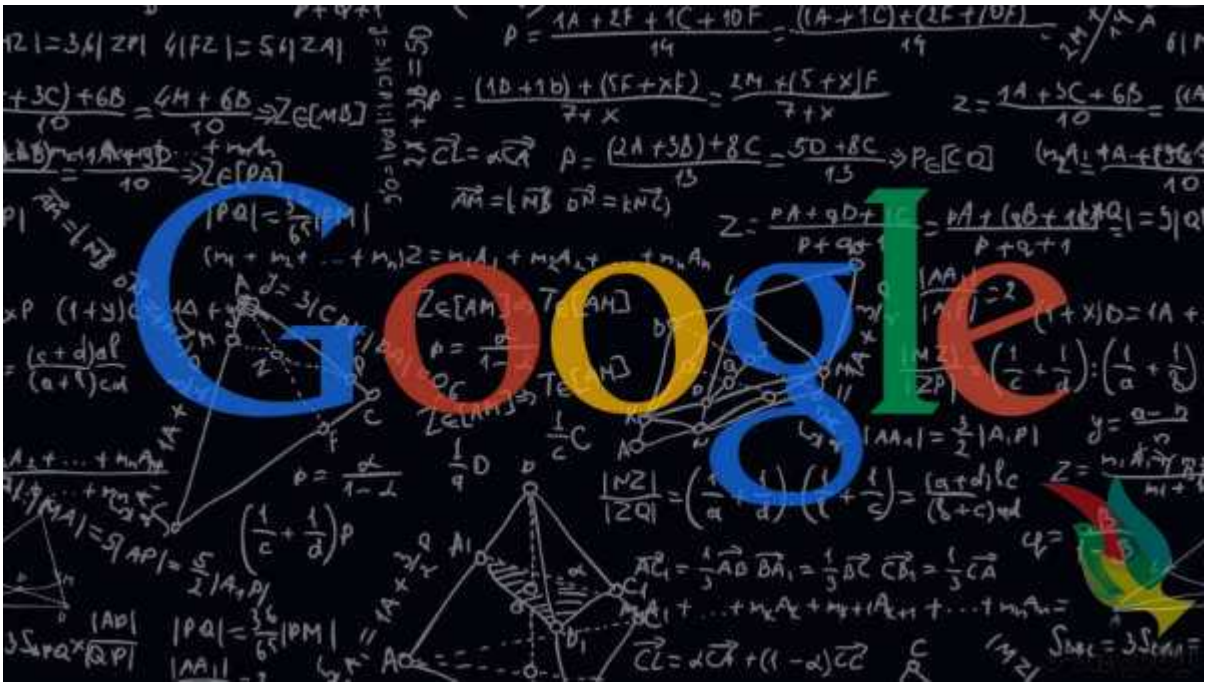
در میان موارد فوق، حداقل سرعت ۱ گیگابیت بر ثانیه که چند برابر بیشتر از سرعت LTE است، تأخیر زیر ۱ میلی‌ثانیه و مصرف انرژی بهینه‌تر، بسیار مهم هستند. در حقیقت شبکه‌ی ۵G تنها برای تجربه‌ی سرعت بالاتر معرفی نمی‌شود بلکه قرار است وسایل هوشمند منزل، محیط کار و شهر را وارد شبکه‌ای بزرگ و گسترده کند.

منبع: مقداد آی تی

گوگل اپلیکیشن هایی که به دنبال دسترسی به اطلاعات اضافه هستند را شناسایی می کند



الگوریتم یادگیری ماشینی جدید گوگل، قادر به شناسایی اپلیکیشن هایی است که به دنبال دسترسی یافتن به اطلاعاتی هستند که حتی نیازی به آنها ندارند. گوگل اخیراً در بلاگ پستی نوشته که اکثر اپلیکیشن های اندرویدی، صرفاً برای سرگرم کردن و یاری رساندن به ما طراحی شده اند و ما اطلاعاتی را دسترس شان قرار می دهیم که به آن نیاز دارند؛ به عنوان مثال، یک اپ دوربین، نیازمند دسترسی به سنسور دوربین و یک اپ جهت یابی، نیازمند دسترسی به سنسور GPS است.



اما اگر یک اپلیکیشن رنگ آمیزی، از شما بخواهد که به لوکیشن، کانکت ها، و میکروفون دسترسی داشته باشد، آن موقع تکلیف چیست؟ قطعاً این اپلیکیشن ها خطرناک هستند و نباید دانلود و نصبشان کرد؛ هرچند که شناسایی آن ها در میان خیل عظیم اپلیکیشن های پلی استور می تواند دشوار باشد.

برای یافتن این اپلیکیشن ها، گوگل قصد دارد نرم افزارهای مشابه را گروه هایی دسته بندی کند و سپس به مقایسه تمام اپلیکیشن های آن دسته از منظر ویژگی هایی که می خواهند به آنها دسترسی یابند

می پردازد. به عنوان وقتی چند اپلیکیشن پیام رسان به دنبال دسترسی به ۸ جواز مختلف هستند و چند اپلیکیشن دیگر، تنها سه یا چهار جواز را طلب می کنند، گوگل متوجه می شود یک مشکلی وجود دارد.

به همین دلیل گوگل الگوریتمی مبتنی بر یادگیری ماشینی توسعه داده که می تواند این دسته بندی را به وجود آورده و نه تنها با شباهت کارکرد اپ های مختلف، بلکه از طریق متادیتا هایی نظیر توضیحات و نمرات کاربران، دقت دسته بندی ها را افزایش دهد. در نهایت اپلیکیشن هایی که خطر کمتری برای کاربران دارند، بالاتر از سایرین به نمایش در می آیند.

منبع:دیجیاتو