محبوب‌ترین شغل‌های حوزه IT در سال ۲۰۲۵

دنیای فناوری اطلاعات (IT) به سرعت در حال پیشرفت است و هر ساله شغل‌های جدید و هیجان‌انگیزی به این حوزه اضافه می‌شوند. در سال ۲۰۲۵، با توجه به رشد تکنولوژی‌های مدرن مثل هوش مصنوعی، بلاکچین، و امنیت سایبری، تقاضا برای متخصصان فناوری به اوج خود می‌رسد. در ادامه، محبوب‌ترین شغل‌های IT و توضیحات آن‌ها را بررسی می‌کنیم:

۱. متخصص هوش مصنوعی (AI Specialist)

متخصصان هوش مصنوعی روی طراحی الگوریتم‌ها و مدل‌های یادگیری ماشین کار می‌کنند که توانایی تصمیم‌گیری یا پیش‌بینی داشته باشند. این افراد در پروژه‌هایی مثل ربات‌ها، سیستم‌های توصیه‌گر (مثل پیشنهاد فیلم یا محصولات)، و خودروهای خودران فعالیت می‌کنند. آینده این شغل درخشان است، چرا که صنایع مختلف مثل سلامت، بانکداری، و حتی آموزش به سرعت در حال استفاده از هوش مصنوعی هستند. انتظار می‌رود این حوزه تا سال‌های آینده یکی از پردرآمدترین مشاغل IT باقی بماند.

۲. تحلیل‌گر داده (Data Analyst)

تحلیل‌گر داده وظیفه دارد اطلاعات خام را به گزارش‌ها و تحلیل‌های مفید تبدیل کند. این کار شامل پاک‌سازی داده‌ها، ایجاد داشبوردهای تحلیلی، و پیشنهاد راهکارهای استراتژیک به شرکت‌هاست. شرکت‌ها به شدت به تحلیل‌گرانی نیاز دارند که بتوانند از داده‌ها ارزش خلق کنند، به‌خصوص در بازاریابی، مدیریت زنجیره تأمین، و مالی. آینده این شغل درخشان است، زیرا با رشد حجم داده‌ها، تقاضا برای تحلیل‌گران حرفه‌ای افزایش خواهد یافت.

۳. مهندس امنیت سایبری (Cybersecurity Engineer)

این افراد مسئول طراحی، پیاده‌سازی، و مدیریت راهکارهایی برای محافظت از داده‌ها و سیستم‌های شرکت‌ها هستند. کارشان شامل شناسایی نقاط ضعف شبکه‌ها، مقابله با حملات سایبری، و آموزش پرسنل درباره تهدیدات سایبری می‌شود. با افزایش تهدیدات امنیتی، شرکت‌ها نیاز بیشتری به این متخصصان پیدا می‌کنند. آینده این شغل بسیار روشن است، چرا که امنیت سایبری به یک ضرورت برای هر شرکت تبدیل شده است.

۴. توسعه‌دهنده بلاکچین (Blockchain Developer)

توسعه‌دهندگان بلاکچین سیستم‌هایی غیرمتمرکز ایجاد می‌کنند که اطلاعات را امن و تغییرناپذیر ذخیره کنند. این تکنولوژی فراتر از ارزهای دیجیتال در زمینه‌هایی مثل قراردادهای هوشمند، ثبت اسناد، و زنجیره تأمین استفاده می‌شود. آینده این شغل با گسترش پذیرش بلاکچین در صنایع مختلف بسیار امیدوارکننده است. متخصصان این حوزه تقاضای زیادی در بانکداری، سلامت، و حتی دولت‌ها دارند.

۵. طراح تجربه کاربری (UX Designer)

طراحان UX مسئول ایجاد تجربه‌ای روان و جذاب برای کاربران در وب‌سایت‌ها و اپلیکیشن‌ها هستند. آن‌ها با تحلیل نیازهای کاربران و طراحی رابط‌های کاربری کار می‌کنند تا محصولاتی قابل‌فهم و کاربرپسند ارائه دهند. این شغل با رشد تجارت الکترونیک و اپلیکیشن‌های موبایل، تقاضای زیادی پیدا کرده است. آینده این شغل درخشان است، زیرا شرکت‌ها به‌طور مداوم به دنبال ارتقای تجربه کاربری محصولات خود هستند.

۶. مهندس رایانش ابری (Cloud Engineer)

این افراد سیستم‌های ابری را طراحی، مدیریت، و بهینه‌سازی می‌کنند تا شرکت‌ها بتوانند به جای سرورهای محلی از خدمات ابری استفاده کنند. کارشان شامل انتقال داده‌ها به ابر، مدیریت منابع ابری، و تضمین امنیت اطلاعات است. با گسترش شرکت‌های دیجیتال، مهندسان ابری نقش حیاتی در IT پیدا کرده‌اند. آینده این شغل روشن است، چرا که بیشتر شرکت‌ها به سمت خدمات ابری حرکت می‌کنند.

۷. توسعه‌دهنده اپلیکیشن‌های موبایل (Mobile App Developer)

این شغل شامل طراحی و ساخت اپلیکیشن‌هایی برای سیستم‌عامل‌های Android و iOS است. توسعه‌دهندگان موبایل باید اپلیکیشن‌هایی با عملکرد سریع، طراحی زیبا، و تجربه کاربری جذاب ایجاد کنند. با گسترش استفاده از گوشی‌های هوشمند، تقاضا برای این حرفه به شدت افزایش یافته است. آینده این شغل تضمین‌شده است، زیرا کسب‌وکارها برای رسیدن به کاربران خود به اپلیکیشن‌های اختصاصی نیاز دارند.

۸. مهندس یادگیری عمیق (Deep Learning Engineer)

مهندسان یادگیری عمیق از شبکه‌های عصبی مصنوعی برای ایجاد مدل‌های پیشرفته استفاده می‌کنند. کار آن‌ها شامل تحلیل تصاویر، پردازش زبان طبیعی، و توسعه سیستم‌های تشخیص گفتار است. این حوزه بسیار پویا و در حال رشد است، چرا که کاربردهای یادگیری عمیق در صنایع مختلف مثل سلامت، حمل‌ونقل، و تبلیغات روزبه‌روز افزایش می‌یابد. آینده این شغل بسیار روشن است و حقوق بالایی هم دارد.

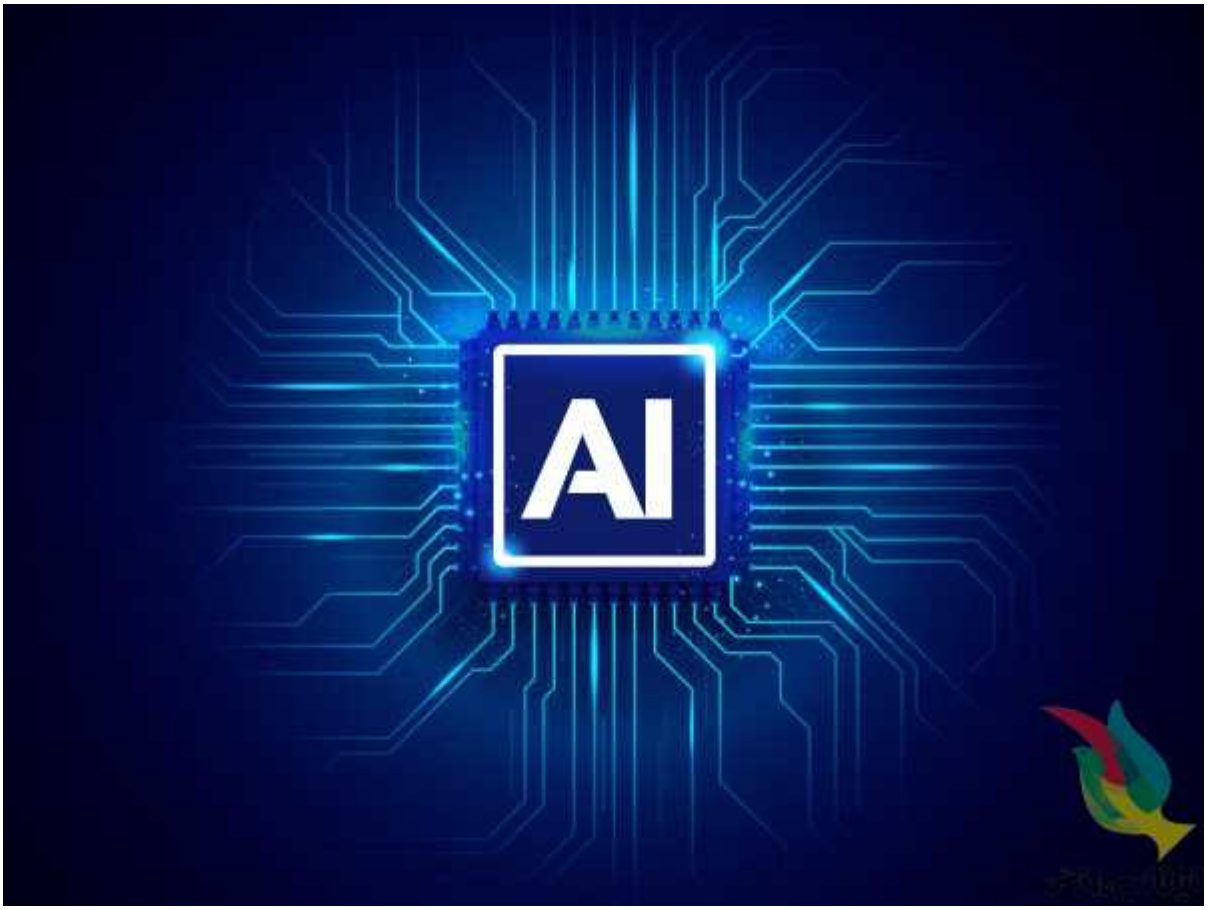
۹. مدیر پروژه فناوری اطلاعات (IT Project Manager)

مدیران پروژه IT وظیفه دارند پروژه‌های فناوری را از مرحله برنامه‌ریزی تا اجرا مدیریت کنند. این شامل مدیریت منابع، زمان‌بندی، و ارتباط با تیم‌های مختلف برای اطمینان از موفقیت پروژه است. این شغل برای شرکت‌هایی که پروژه‌های پیچیده فناوری دارند حیاتی است. آینده این حرفه با رشد پروژه‌های فناوری و نیاز به مدیریت بهتر بسیار روشن است.

۱۰. توسعه‌دهنده واقعیت افزوده و مجازی (AR/VR Developer)

این توسعه‌دهندگان اپلیکیشن‌ها و سیستم‌هایی ایجاد می‌کنند که از واقعیت افزوده و مجازی برای آموزش، بازی، یا شبیه‌سازی استفاده می‌کنند. آن‌ها از ابزارهایی مثل Unity و Unreal Engine برای طراحی محیط‌های دیجیتالی استفاده می‌کنند. آینده این حرفه با ورود این تکنولوژی‌ها به صنایع مختلف مثل آموزش، پزشکی، و معماری بسیار روشن است.

آینده هوش مصنوعی در زندگی انسان



هوش مصنوعی (AI) به عنوان یکی از مهمترین تحولات فناوری در قرن بیست و یکم، زندگی روزمره انسان‌ها را تغییر داده است.

در این مقاله قصد داریم به بررسی تأثیرات هوش مصنوعی بر زندگی انسان‌ها، چالش‌ها، و چشم‌اندازهای آینده آن بپردازیم.

تاریخچه‌ای از هوش مصنوعی

تاریخ هوش مصنوعی به دهه‌های ۱۹۵۰ و ۱۹۶۰ برمی‌گردد، زمانی که پژوهشگران به دنبال ساخت ماشین‌هایی بودند که بتوانند کارهایی انجام دهند که نیاز به هوش انسانی دارد.

آلن تورینگ با پیشنهاد «آزمون تورینگ» به ارزیابی هوش ماشین‌ها کمک کرد. با پیشرفت زبان‌های برنامه‌نویسی و الگوریتم‌های یادگیری ماشین در دهه‌های بعد، هوش مصنوعی به تدریج در کاربردهای عملی مانند پردازش زبان طبیعی، تشخیص تصویر و رباتیک گسترش یافت.

امروزه، به لطف توان محاسباتی بالا و داده‌های کلان، شاهد جهش‌های قابل توجهی در این زمینه هستیم.

جنبه‌های مختلف هوش مصنوعی

۱_ بهداشت و درمان

– تأثیر هوش مصنوعی در تشخیص و درمان بیماری‌ها.
– سیستم‌های هوشمند مدیریت بیمارستان و صورت‌حساب‌ها.
– کاربردهای هوش مصنوعی در تحقیق و توسعه دارو.

۲_ آموزش

– استفاده از هوش مصنوعی برای شخصی‌سازی تجربه یادگیری.
– ابزارهای هوشمند برای ارزیابی عملکرد دانش‌آموزان.
– نقش هوش مصنوعی در برقراری ارتباط میان معلمان و دانش‌آموزان.

۳_ حمل و نقل

– خودروهای خودران و تأثیر آن‌ها بر ایمنی و ترافیک.
– امکان ایجاد سیستم‌های حمل و نقل عمومی هوشمند.

۴_ صنعت و اقتصاد

– کاربردهای هوش مصنوعی در بهینه‌سازی فرایندهای صنعتی.
– تأثیر بر بهره‌وری و کاهش هزینه‌ها در تولید.

۵_ سرگرمی و رسانه

– استفاده از هوش مصنوعی در تولید محتوا و سرگرمی.
– تأثیر توصیه‌گرها بر رفتار مصرف‌کننده.

۶_ کشاورزی

– نقش هوش مصنوعی در بهینه‌سازی روش‌های کشاورزی و افزایش تولید.

چالش‌ها و موانع

۱_ نگرانی‌های اخلاقی

– مسائل مربوط به تصمیم‌گیری هوش مصنوعی و مسئولیت‌پذیری.

۲_ امنیت و حریم خصوصی

– مشکلات ناشی از جمع‌آوری و ذخیره‌سازی داده‌ها و حفظ حریم خصوصی.

۳_ اشتغال و کارآفرینی

– تأثیر خودکارسازی بر بازار کار و مشاغل.

۴_ تبعیض و نابرابری

– چالش‌های مربوط به ایجاد الگوریتم‌های عادلانه و بدون تبعیض.

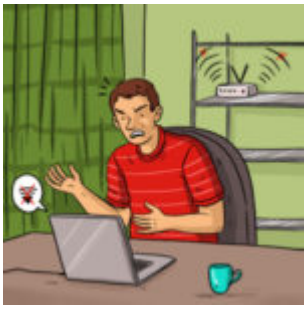
۵_ وابستگی به فناوری

– مشکلات ناشی از وابستگی جوامع به سیستم‌های هوش مصنوعی.

منابع

– Russell, S., & Norvig, P. (2016). *Artificial Intelligence: A Modern Approach.*
– Tegmark, M. (2017). *Life 3.0: Being Human in the Age of Artificial Intelligence.*
– Bostrom, N. (2014). *Superintelligence: Paths, Dangers, Strategies.*
– Shirky, C. (2010). *Cognitive Surplus: Creativity and Generosity in a Connected Age.*
– از مقالات و منابع آنلاین معتبر در زمینه هوش مصنوعی و تکنولوژی.

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.

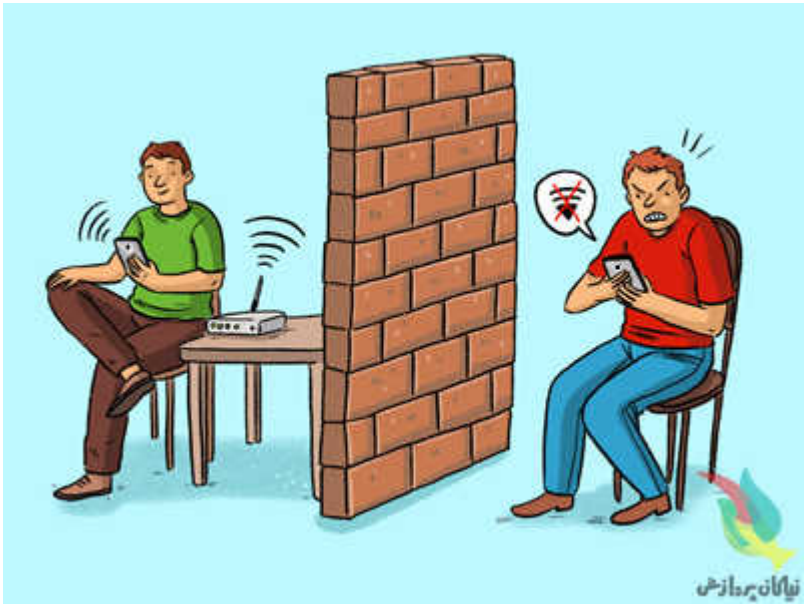
در این مطلب به شما می گوییم دشمنان اصلی WiFi کدام آیتم هستند. نکات مفیدی را در انتهای مقاله خواهید یافت که می توانید از آنها برای جلوگیری از آنتن دهی ضعیف استفاده کنید ، آنها را از دست ندهید!

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.

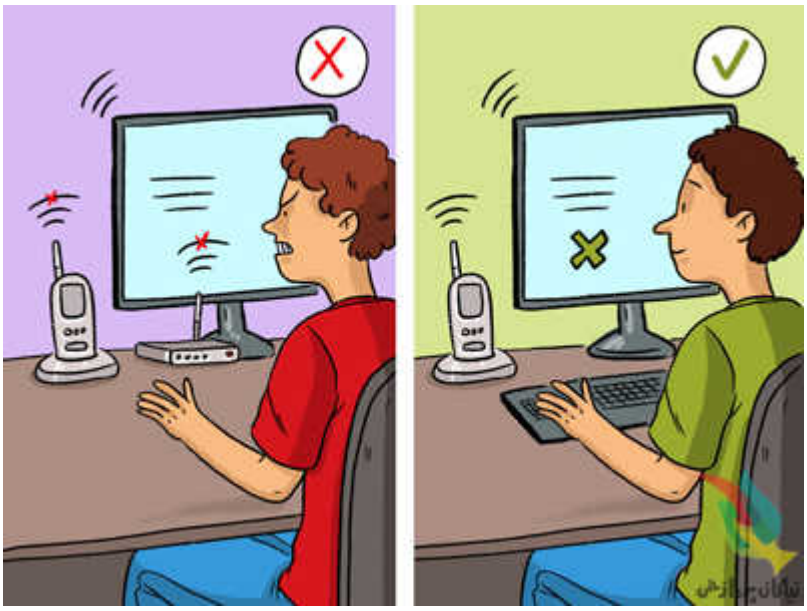
۴-یخچال و ماشین لباسشویی

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.

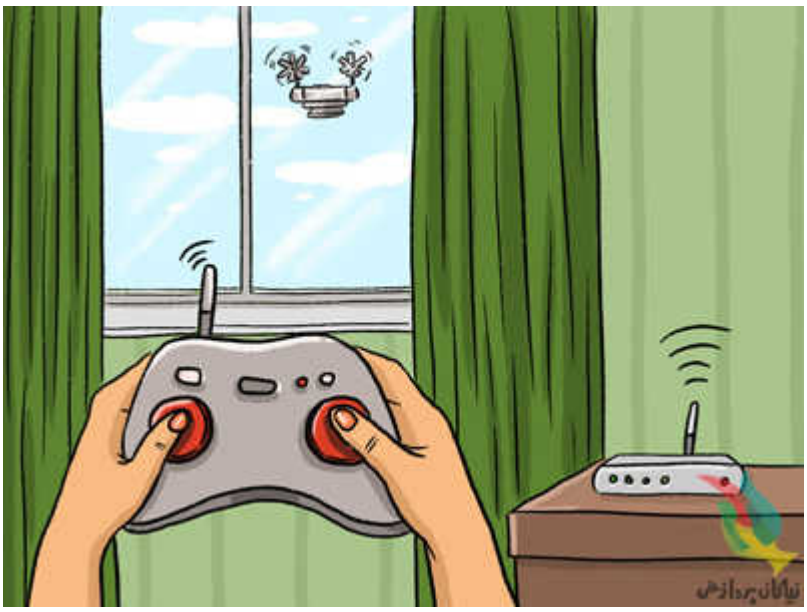
۶-مانیتور کودک



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



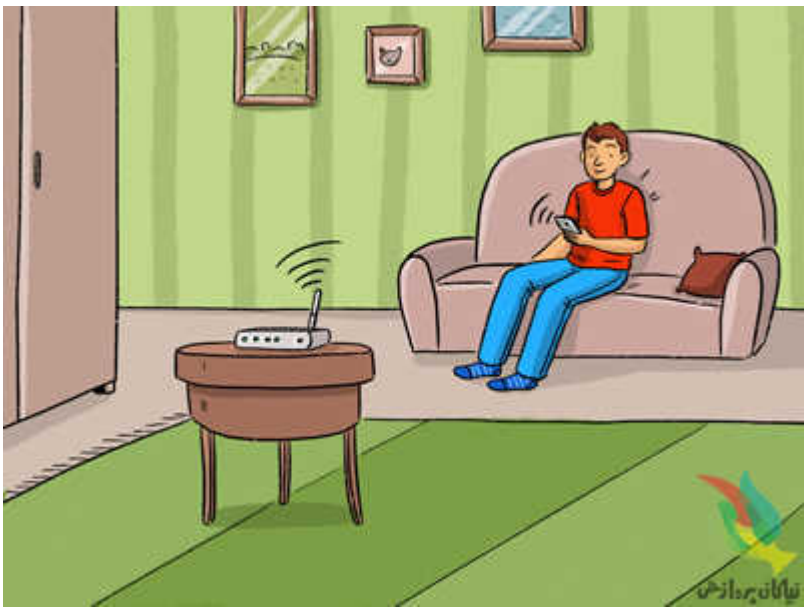
هواپیماهای بدون سرنشین همچنین با سرعت ۲٫۴ گیگاهرتز کار می کنند ، اما همه مدل ها این اختلال را ایجاد نمی کنند. همه اینها به میزان توان مورد نیاز هر مدل بستگی دارد.

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.

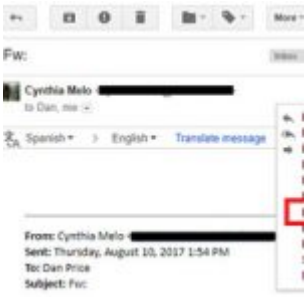
6. فقط از جدیدترین و مدرن ترین فن آوری های WiFi استفاده کنید.
7. پهنای باند هایی که در ۵ گیگاهرتز کار می کنند ، معمولاً ارتباطی بسیار سریعتر از سایرین ارائه می دهند ، زیرا این کانال کمتر از باند ۲٫۴ گیگاهرتزی شلوغ است.

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

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

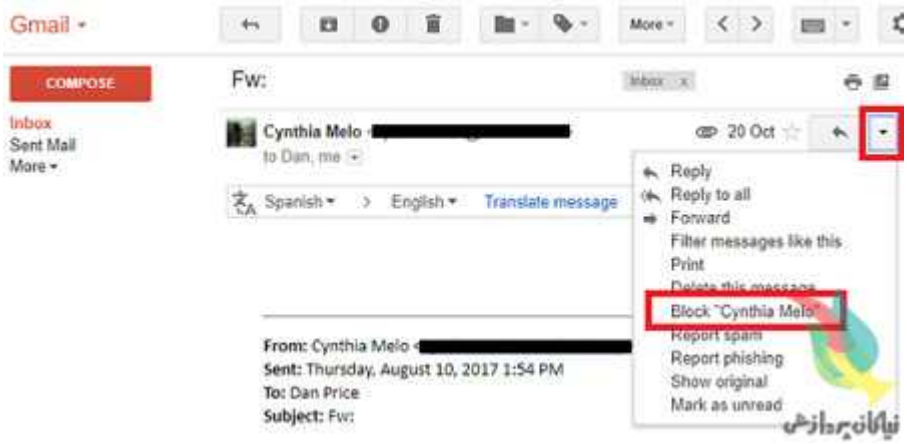
۱- در مرورگر خود به‌مسیر google.com/gmail بروید و با تایپ نام کاربری و گذرواژه وارد حساب کاربری‌تان شوید.

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

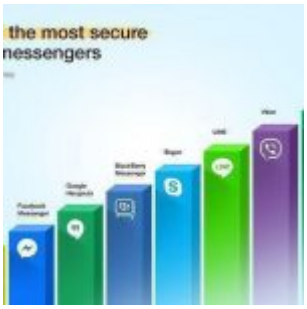
با توجه به هزینه بالای ترجمه شاید برای بسیاری از دانشجویان مراجعه به دارالترجمه‌ها مقرون به صرفه نباشد. برای حل این مشکل فارسیز، ترجمه دانشجویی با کیفیت برنزی و نقره‌ای که اقتصادی و به صرفه است را پیشنهاد می‌کند. وقتی **ترجمه مقاله** و متون انگلیسی را به فارسیز می‌سپارید از کیفیت ترجمه مطمئن باشید زیرا 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

ده مسنجر معتبر و امن دنیا !!!



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.

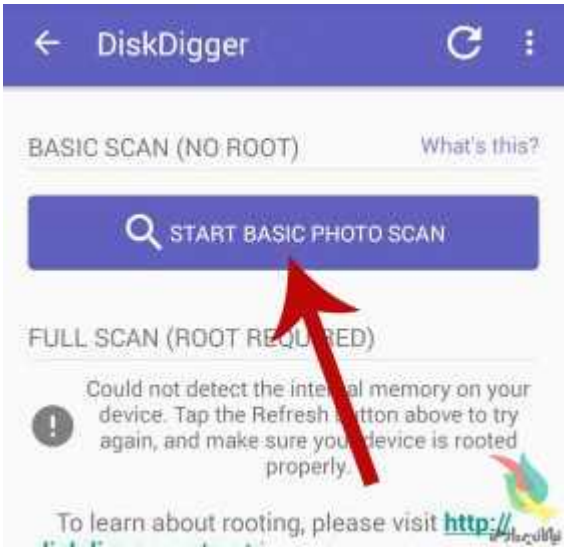
برای انجام این کار در گوشی‌های اندرویدی مراحل زیر را به ترتیب طی کنید:

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!

حملاتی که به گوشی های هوشمند انجام میشود

تشریح نفوذ به یک دستگاه تلفن همراه

چگونه یک هکر می‌تواند از گوشی شما سو 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.

نظارت

- صدا
- دوربین
- لیست تماس
- موقعیت مکانی
- پیامک‌ها

جعل هویت

- فرستادن پیامک‌های شما
- ارسال پیام‌های ایمیل
- ارسال بر روی شبکه‌ی اجتماعی شما

سرقت اطلاعات

- اطلاعات حساب کاربری
- لیست ارتباطات
- لیست تماس‌ها
- شماره تلفن
- دزدیدن اطلاعات توسط برنامه‌های آسیب‌پذیر
- سرقت شماره سریال دستگاه (IMEI)

زیان مالی

- ارسال پیام نرخ حق بیمه
- دزدیدن شماره تراکنش احراز هویت (TANs)
- اخاذی توسط برنامه‌های مخرب
- شماره تلفن
- آنتی ویروس تقلبی
- برقراری تماس‌های گران‌قیمت

فعالیت‌های خودکار مخرب

- اجرای برنامه‌های هک
- تبلیغات مزاحم
- ارسال پیام نرخ حق بیمه

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

۱۱۳ گوشی هوشمند در امریکا در هر دقیقه گم می‌شود.

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

۳۵۰،۰۰۰ ویروس اندرویدی توسط SophosLabs دیده شده‌است.

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 عموما با پیشنهادهای مهیجی از قبیل برنده شدن در یک مسابقه یا … می باشد. توجه داشته باشید اینگونه ایمیل ها عموما از آدرس دوستان شما که هک شده اند برای شما ارسال می شود.

۳ – بر روی لینک های خبرهای مهیج مخصوصا 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 کنید. 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.