افزایش کیفیت و محدوده شبکه بی‌سیم

استفاده از شبکه بی‌سیم این روزها دیگر خیلی ساده شده است. تنها کافی است یک روتر بیسیم را خریداری کنید و سپس پورت اینترنت آن را به دستگاه مودم ADSL خود وصل کنید. حال می توانید از تمامی دستگاه ها و سیستم هایی که در اختیار دارید به روتر خود وصل شوید و از اینترنت در تمامی آن سیستم ها استفاده کنید.

اما با وجود رشد استفاده از شبکه های بی سیم در خانه ها و شرکت ها بعضی از کاربران از کیفیت و محدوده‌ای که می توانند با آن به شبکه های بی سیم اتصال پیدا کنند ناراضی هستند. در این آموزش از تورتک با هم یاد می گیریم که چگونه شبکه بی‌سیم خانگی خود را تقویت کرده و با این کار کیفیت دریافت سیگنال و محدوده قابل دسترس بودن سیگنال ها را افزایش دهیم.

چگونگی تقویت قدرت سیگنال های WiFi شبکه بی‌سیم

قبل از اینکه با انجام ترفندهایی قدرت و محدوده سیگنال های شبکه بی‌سیم خود را افزایش دهیم بهتر از با نکته‌ای آشنا شوید که در هنگام خرید روترهای خانگی به آن نیاز دارید. در هنگام خرید دستگاه روتر توجه داشته باشید که دستگاه مورد نظر از ارتباط بر مبنای استاندارد ۸۰۲.۱۱n پشتیبانی کند. در اینگونه ارتباط برخلاف نسخه قدیمی تر خود یعنی ۸۰۲.۱۱g که در بازار ایران نیز به راحتی پیدا می شود قدرت سیگنال و همچنین سرعت تبادل اطلاعات تغییر چشمگیری کرده است و شما با در اختیار داشتن یک روتر بر پایه ۸۰۲.۱۱n کمتر به مشکلاتی مانند قطعی در هنگام تبادل فایل های حجیم و ویدئو ها در بین دستگاه های متصل به شبکه بر می‌خورید.

اما در هر صورت ترفندهایی نیز برای افزایش کیفیت و محدوده سیگنال دهی شبکه های بی‌سیم خانگی وجود دارد که با آن ها در زیر آشنا می شویم.

1. **استفاده از DD-WRT :** در صورتی که نام مودم و یا دستگاه روتر شما در لیست دستگاه های سازگار با DD-WRT firmware وجود داشته باشد (مشاهده لیست) می توانید با دانلود این firmware (لینک دانلود DD-WRT) و نصب آن از طریق پنل مدیریتی روتر خود حداقل چند متری را به محدوده شبکه بیسیم خود اضافه کنید و با این کار همچنین کیفیت سیگنال های شما هیچ تغییر خاصی نیز نمی کنند. در صورتی که دستگاه شما با این firmware سازگاری نداشت پیشنهاد می کنم از Tomato firmware استفاده کنید.
2. **استفاده از ورق های آلمینیومی :** اکثر روترها بر روی خود یک آنتن دارند که اطلاعات و سیگنال ها را به تمامی جهت های ممکنه ارسال می کنند مانند یک لامپ معمولی که نور را پخش می کند. در صورتی که از دستگاه روتر خود در مرکز محدوده و یا خانه خود استفاده می کنید این ویژگی می تواند خیای مفید باشد اما اگر روتر شما در گوشه ای از خانه شما قرار دارد می توانید با استفاده از یک ورق آلمینیومی و حتی یک قوطی نوشابه آهنی باز شده بین دیوار و دستگاه روتر خود از هدر رفتن سگنال‌ها جلوگیری کنید و آن ها را دوباره به سمت محدوده کاری خود برگردانید. البته اگر می خواهید بهترین

نتیجه ممکنه را از این ترفند بگیرید بهتر است کمی بر روی حالت ورق آلمینیومی در پشت روتر خود کار کنید و با انتخاب شکل های مختلف به بهترین حالت ممکن دست یابید.

3. **استفاده از نرم افزار InSSIDer :** این نرم افزار کاملاً رایگان می تواند وجود و قدرت سیگنال های شبکه بی‌سیم خانگی شما را نمایش دهد. بهتر است این نرم افزار را بر روی لپ تاپ خود نصب بکنید و سپس در نقاط مختلف خانه از دسترسی و کیفیت سیگنال های شبکه با خبر شوید. با کنار هم گذاشتن اطلاعات به دست آمده خود می توانید بهترین مکان قرار گیری دستگاه روتر را تشخیص دهید. برای دانلود این نرم افزار از لینک InSSIDer استفاده کنید.
4. **انتخاب بهترین مکان برای روتر :** یکی دیگر از مواردی که می‌تواند در بهبود کیفیت و محدوده شبکه های بیسیم تاثیر بگذارد انتخاب یک مکان صحیح برای دستگاه روتر شبکه شما است. توجه داشته باشید که در کنار روتر بی سیم خود نباید دستگاه بی‌سیم دیگری وجود داشته باشد و سعی کنید از اجسام آهنی که ممکن است سیگنال ها را در جهت بی استفاده ای بازتاب کنند دستگاه روتر شما دور باشد. همچنین سعی کنید در وسط محل استفاده از شبکه بی سیم و همچنین در نقطه بالایی نسبت به دیگر دستگاه ها روتر شما قرار بگیرد.
5. **استفاده از آنتن‌های uni-directional :** معمولاً دستگاه های روتر با یک آنتن از نوع omni-directional که کیفیت معمولی نیز دارد فروخته می شوند ، پس اگر می خواهید محدوده و جهات پخش شدن سیگنال های شبکه بی‌سیم خود را افزایش دهید می توانید با خرید یک آنتن uni-directional قوی‌تر و نصب آن بر روی دستگاه روتر خود این کار را انجام دهید. اگر آنتن بهتری را در بازار برای خرید پیدا نکردید حداقل می توانید از آنتن های بهتر از مدل فعلی آنتن روتر خود که از تکنولوژی omni-directional در آن ها استفاده می شود را به راحتی پیدا کنید.

افزایش محدوده شبکه های بی‌سیم با

استفاده از سخت افزارهای جانبی

یکی دیگر از مواردی که کاربران شبکه های بی سیم خانگی به آن نیاز پیدا می کنند این است که محدوده قابل دسترس بودن شبکه خود را افزایش دهند که برای اینکار بهترین روش ممکن استفاده از سخت افزارهای جانبی است که کمپانی های معروف ارائه می دهند. در زیر با تاثیر گذار ترین روش های ممکن برای افزایش محدوده شبکه های بیسیم WiFi آشنا می شویم.

1. **استفاده از دستگاه WiFi Repeater :** این دستگاه همانطور که از اسم آن پیدا است قابلیت این را دارد که سیگنال های ارسالی دستگاه روتر بی سیم شما را دریافت کند و آن ها را با کیفیت و قدرت اولیه در محدوده ای که قرار دارد دوباره در تمامی جهات بحش کند. بهترین حالت استفاده از این دستگاه در زمانی است که آن را در نقاطی قرار دهیم که بعد از آن ها دیگر سیگنال های دستگاه روتر ما در دسترس نیست تا بتوانیم محدوده شبکه خود را بدون نیاز به هیچ سیمی افزایش دهیم.
2. **استفاده از یک روتر دیگر :** یکی دیگر روش هایی که برای افزایش محدوده های شبکه بی سیم به شما پیشنهاد می کنیم خرید و استفاده از یک روتر دیگر در کنار روتر فعلی شما است. تنها کافی است روتر اصلی خود را به اینترنت متصل کنید اگر می خواهید در شبکه اینترنت قابل دسترس باشد و سپس با یک کابل به شیوه LAN دستگاه روتر دوم را به روتر اصلی وصل کنید. جالب است بدانید در این روش می توانید تا ۱۰۰ پا دورتر دستگاه روتر دوم را قرار دهید چون برای دریافت اطلاعات از شبکه شما از یک سیم استفاده می شود.
3. **استفاده از یک Access Point :** با استفاده از یک دستگاه Access Point نیز می توانید به محدوده شبکه بی سیم خود وسعت بیشتری را بدهید مانند استفاده از WiFi Repeater که در بالا با آن آشنا شدیم. از مزایای این روش می توان به قابلیت اتصال سیستم های بیشتر به شبکه و از معایب آن می توان به قیمت بالای این دستگاه نسبت به یک روتر اشاره کرد.

آموزش رمز گذاری اسناد در word

ویژگی‌های جدید Office 2007 مانند امضای دیجیتالی و رمزگذاری به شما کمک می‌کنند تا اطلاعات محرمانه خود را قفل کرده و دور از چشمان جست‌وجوگر دیگران نگه دارید.

نرم‌افزار Word به عنوان اصلی‌ترین ابزار ایجاد اسناد، از هر ۹ کاربر ۵ نفر را به خود اختصاص می‌دهد و به کاربران این فرصت را می‌دهد تا در اسرع وقت نامه‌های مشتریان، گزارشات مالی رؤسا و حتی پروژه‌های عظیم اجرایی را آماده کنند.

اما حتی در عصر شبکه‌های بی‌سیم و با وجود برنامه‌های جاسوسی، بسیاری از افراد، اطلاعات حساس و مهم خود را بدون حفاظت رها می‌کنند.

نگران نباشید. ویژگی‌های جدید Office 2007 مانند امضای دیجیتالی و رمزگذاری به شما کمک می‌کنند تا اطلاعات محرمانه خود را قفل کرده و دور از چشمان جست‌وجوگر دیگران نگه دارید.

امضای اسناد

نرم‌افزار Word 2007 یک ویژگی جدید امنیتی را برای اسناد، ارائه کرده است و آن امضای دیجیتالی است. شما می‌توانید به هر سند یک فیلد امضا اضافه کنید و به این ترتیب، فایل قفل شده و امکان انجام هیچ ویرایشی روی آن وجود نخواهد داشت؛ مگر اینکه امضای دیجیتالی حذف شود.

ممکن است هر فردی قادر به حذف امضا و ویرایش فایل باشد، اما سند امضا شده، مهر تائید شماست.

استفاده از رمزگذاری و کلمه عبور

امضای دیجیتالی، سند را در مقابل ایجاد تغییرات، حفاظت می‌کند و در واقع به آن اعتبار می‌بخشد؛ خصوصاً اگر از تصویر bitmap امضای حقیقی خود استفاده کنید. اما هنوز این امکان وجود دارد که اسناد امضا شده، باز و خوانده شود. بنابراین استاندارد AES (استاندارد رمزگذاری پیشرفته) به همراه یک کلید ۱۲۸ بیتی و SHA-1 به Word 2007 اضافه شده است. باید به این نکته توجه کنید که اگر سند موردنظر را به صورت دیجیتالی امضا کرده‌اید، دیگر حتی با اضافه کردن یک کلمه عبور هم نمی‌توانید آن را تغییر دهید.

فقط اسناد امضا نشده می‌توانند توسط کلمه عبور حفاظت شوند. روی دکمه Office در قسمت بالای سمت چپ کلیک کنید، سپس گزینه Prepare و Encrypt Document را انتخاب کنید. کلمه عبوری را انتخاب کنید که حدس زدن آن دشوار باشد. از حروف کوچک و بزرگ و اعداد بهره گیرید

و برای برخورداری از بالاترین میزان حفاظت، حداقل از ۸ کاراکتر استفاده کنید. حال روی OK کلیک کنید.

کلمه عبور را مجدداً وارد کنید. حال اگر هر فردی سند موردنظر را باز کند، باید کلمه عبور مربوطه را تایپ کند؛ در غیر این‌صورت دستیابی به متن غیر ممکن است.

به منظور اضافه کردن امضای دیجیتالی، ابتدا سند موردنظر را باز و یا ایجاد کنید. سپس روی زبانه Insert کلیک کرده و گزینه Signature Line در سمت راست را انتخاب کنید. روی OK کلیک و سپس مواردی از قبیل اسم، عنوان و آدرس پست الکترونیکی شخص امضا کننده (خودتان) را پر کنید. شما حتی قادرید تاریخ را هم به امضای خود اضافه کنید. سپس روی دکمه OK کلیک کنید. برای امضای سند، روی محل امضا دابل کلیک کنید. اسمتان را تایپ یا روی Select Image کلیک کنید تا فایل bitmap امضای حقیقی خود را انتخاب کنید. سپس روی Sign کلیک کنید.

از بخش‌های مهم سند حفاظت کنید

ممکن است فایل موردنظر خود را امضا و یا رمزگذاری کرده باشید اما تصمیم بگیرید که به دیگران اجازه دهید متن موردنظر شما را ویرایش کنند، اما این تغییرات کاملاً تحت کنترل شما باشد. در این حالت چه کار باید کرد؟ روی گزینه Review و سپس Protected Document (در قسمت راست) کلیک کنید و گزینه‌های قالب‌بندی را که دیگران می‌توانند ویرایش کنند، انتخاب کنید. برای مثال شما می‌توانید این اختیار را به آنها بدهید که مثلاً فونت را تغییر دهند ولی در اندازه آن تغییری ایجاد نکنند. همچنین شما می‌توانید از Track Changes استفاده کنید. در این صورت ویرایش صورت گرفته به صورت متمایز نمایش داده می‌شود. برای حفاظت از سند، گزینه Start Enforcing را انتخاب کرده و سپس رمز عبور را وارد و بعد تائید کنید.

تفاوت های گوگل پلاس با فیس بوک

وقتی مردم سئوال "آیا Google+ می تواند Facebook را مغلوب کند؟" را بیان می کنند یک موضوع را مدنظر قرار نداده اند. در واقع رقابت آغاز شده، جنگ میان دو وب سایت نیست Google+ فراتر از یک سایت است. دلیلی که گوگل این پروژه را Google+ Project می نامد این است که Google+ در آینده به بخش اصلی هویت گوگل تبدیل می شود و کل شرکت را تغییر شکل می دهد. پس بهتر است بپرسیم آیا گوگل می تواند فیس بوک را شکست دهد؟ البته فیس بوک بسیار قوی تر از آن است که Google+ بتواند به راحتی آن را مغلوب کند ولی Google+ امکانات جذابی دارد که ممکن است باعث پیروزی آن شود.

در ادامه ۹ مزیت و برتری Google+ نسبت به Facebook را ملاحظه خواهید کرد:

یکپارچه سازی با سرویس های مختلف گوگل

۱- مهمترین برتری Google+ در یکپارچگی آن با سرویس های متنوع گوگل است تمام سرویس های گوگل از جستجو در اسناد و ویدیوها تا Picasa به شبکه اجتماعی Google+ متصل هستند. Google+ همچنین در نوار بالای سرویس های گوگل قرار دارد و کاربر را از وقایع اتفاق

افتاده با خبر می سازد تا کاربر در تمام سرویس های گوگل به سرعت به آنها دسترسی داشته باشد. Google+ در سمت راست نوار مشکی هدایت کننده گوگل قرار دارد و کاربر را از پیغام ها، بروز رسانی ها و وقایع مطلع می کند. در حال حاضر سرویس های مختلف گوگل از Gmail, Docs تا موتور جستجو میلیون ها کاربر دارند و این کاربرها راحتر از Google+ استفاده خواهند کرد.

مدیریت بهتر دوستان

۲- Google+ دارای امکان بسیاری دوست داشتنی به نام Circles است که کاربر از طریق آن می تواند به راحتی دوستان خود را در حلقه های متفاوت دسته بندی کند تا محتوای مورد نظر را تنها بین افراد یک حلقه به اشتراک بگذارد. کاربر می تواند با دوستان خود در یک حلقه چت و یا مکالمه ویدیوی داشته باشد. در فیس بوک نیز می توان دوستان را در گروه های مختلف دسته بندی کرد ولی گروه ها به هیچ وجه به خوبی حلقه ها نیستند.

نرم افزار بهتر موبایل

۳- اگر شما هم کاربر اندروید هستید یعنی تبلت یا تلفن هوشمند اندرویدی دارید، Google+ نرم افزار بسیار ساده و کارآمدی برای شما دارد با این نرم افزار به راحتی می توانید از امکانات بسیار خوب این شبکه اجتماعی در ابزار موبایل خود استفاده نمایید. گوگل امیدوار است تا کاربران انبوه اندورید را به سمت این شبکه اجتماعی جذب کند و اعلام کرده که د ر آینده امکانات ویژه ایی را برای کاربران اندروید ارائه خواهد کرد.

یافتن ساده محتوا برای اشتراک گذاری

۴- اسپارک (Spark) یکی از امکانات Google+ است که آن را با Facebook متمایز می کند. Spark به دیتابیس غنی گوگل دسترسی دارد و از امکانات موتور جستجوی این شرکت برای یافتن محتوا (عکس، متن، فیلم و غیره) استفاده می کند و محتوا را براساس موارد مورد علاقه کاربر به او پیشنهاد می کند تا به راحتی بین دوستانش به اشتراک بگذارد. این قابلیتی است که Facebook هرگز به آن دست نخواهد یافت چون فیس بوک موتور جستجو ندارد و حتی اگر مایکروسافت بخواهد با آن همکاری کند باز هم موتور جستجوی Bing قابل مقایسه با Google نخواهد بود. با Spark کاربر نیازی ندارد برای یافتن محتوای مورد

نظر خود جستجو کند خود Google+ موارد را به کاربر پیشنهاد می دهد.

می توانید اطلاعات خود را پس بگیرید

۵- فیس بوک به دلیل نحوه نمایش اطلاعات شخصی کاربران بد نام است. در فیس بوک بخشی از اطلاعات کاربر همیشه برای عموم قابل نمایش است و به سختی می توان پروفایل فیس بوک را برای همیشه حذف کرد. اما Google+ این امکان را فراهم کرده است و کاربر می تواند تمام اطلاعات خود را دانلود کرده و پروفایل خود را به همراه تمام اطلاعات آن حذف کند. این امکان توسط ابزاری به نام Data Liberation فراهم شده است. کاربر با چند کلیک ساده کلیه اطلاعات خود شامل تصاویر، ویدیوها، متون، Stream ها، کانتکت ها و غیره را برروی کامپیوتر خود دانلود می کند.

تگ کردن بهتر افراد به تصاویر

۶- زمانی که در Google+ در حال مشاهده تصاویر هستید می توانید افراد را به یک تصویر تگ کنید شبیه کاری که در فیس بوک انجام می دهید. یک مربع کوچک برروی چهره شخص می کشید و سپس نام او را وارد می کنید. اما یک تفاوت عمده در نحوه مدیریت حریم شخصی در گوگل وجود دارد. زمانیکه شما شخصی را به یک تصویر تگ می کنید یک پیغام نمایش داده می شود که در آن به کاربر اعلام می کند: "شخص تگ شده از تگ شدنش در این تصویر مطلع خواهد شد، کاربر تگ شده می تواند به تصاویر مرتبط با این آلبوم دسترسی داشته و آنها را مشاهده کند".

گوگل همچنین از امکان تشخیص چهره خودکار، دوری کرده است در حال حاضر فیس بوک بصورت خودکار چهره افراد موجود در تصاویر آپلود شده کاربر را تشخیص داده و آنها را تگ می کند. گوگل نیز قدرت اعمال چنین امکانی را دارد همانطور که نرم افزار Picasa این کار را به خوبی انجام می دهد ولی از آن پرهیز کرده است.

امکان مکالمه ویدیویی چند نفره

۷- گوگل پلاس برای غلبه بر فیس بوک قابلیت های بسیاری در زمینه چت و مکالمه ارائه کرده است.Google+ علاوه بر امکان چت نوشتاری، مکالمه ویدیوی را نیز به کاربران ارائه می دهد. با Hangout در

Google+ می توان با دوستان، همکاران و یا اقوام خود در یک حلقه گفتگوی ویدیویی چند نفر داشت. Hangout بسیار خوب طراحی شده است و همزان با گفتگوی ویدیوی می توان از گفتگوی نوشتاری نیز استفاده کرد.Hangout علاوه بر استفاده های شخصی می تواند برای جلسات شرکت ها و تشیکلات مختلف استفاده شود. در حال حاضر فیس بوک هیچ سرویش مشابه ایی ندارد ولی شایعات حاکی از آن است که فیس بوک به کمک اسکایپ قصد دارد امکان مکالمه ویدیویی را به Facebook اضافه کند.

اشتراک گذری امن تر محتوا

۸- طرفداران حریم شخصی همواره از شبکه های اجتماعی درخواست دارند تا به کاربران اجازه دهند برای تک تک محتوای به اشتراک گذاشته شده سطح دسترسی تعیین کنند. در حال حاضر در فیس بوک می توانید برای انواع مختلف محتوا دسترسی تعیین کنید ولی نمی توانید برای هر محتوای به اشتراک گذاشته شده سطح دسترسی متفاوتی داشته باشید. اما Google+ این امکان را به کاربر می دهد، کاربر می تواند در زمان به اشتراک گذاری محتوا، حلقه های دوستان خود را نیز انتخاب کند یعنی می تواند یک عکس را تنها برای دوستان یک حلقه به اشتراک بگذارد.

گوگل ناظر بهتری بر اطلاعات شخصی کاربران است

۹- یکی از مهمترین موارد در راه اندازی شبکه اجتماعی حفظ اطلاعات شخصی کاربران می باشد. فیس بوک یک شرکت جوان است که به تازگی رشد کرده و در طی چند سال اخیر اشتباهات زیادی را مرتکب شده است. اما گوگل برخلاف فیس بوک یک شرکت کاملا جا افتاده و شکل یافته ایی است که همواره به حفظ حریم شخصی و محافظت از اطلاعات شخصی کاربران مشهور است. گوگل تحت هیچ شرایطی حاضر به ارائه اطلاعات شخصی کاربران به دولت ها و یا تشکل های مختلف نشده است.

Dropbox 2.6.12 Final فضـــــای رایگان برای ذخیره اطلاعات

Dropbox 2.6.12 Final یک سیستم‌هاست فایل‌ها تحت وب است که با استفاده از سیستم Cloud Computing و دسترسی به اینترنت به شما اجازه می‌دهد تا فایل‌هایتان را به راحتی share کنید(البته در مورد طریقه ی شیر کردن فایل‌ها توضیح داده خواهد شد)

DropBox چگونه کار می‌کند؟

به طور مختصر شما از طریق Browser خود می‌توانید فایل‌هایتان را آپلود کنید و هر وقت و هرجا که خواستید آنها را دانلود کنید.

ابتدا شما باید برنامه Drop Box را از سایتش دانلود کنید. که حجم آن حدود ۱۲ مگابایت است.

سپس برنامه را نصب کنید هنگام نصب برنامه می‌توانید اکانت لازمه را برای خود ثبت کنید.

هنگام نصب می‌توانید محل فولدری که Drop Box می‌سازد تعیین کنید.

همچنین یک آیکون رو دسکتاپتان ظاهر خواهد شد. که با بازکردن آن به فولدر مربوطه می‌روید.

کار با Drop Box ساده تر از آن چیزیست که تصور می‌کنید.

درون فولدر اولیه ۳ فایل راهنما وجود دارد که مراحل کار را توضیح داده. که در اینجا به مراحل کلی کار اشاره می‌کنیم.

قدم اول: هر فایل یا فولدری را که می‌خواهید با انداختن (drag & drop) آن بر روی فولدر drop Box منتقل کنید.

قدم دوم: بعد از انجام مرحله ی اول Drop box شروع به آپلود و منتقل کردن آن به سرورها می‌کند. شما کافیست صبر کنید تا تیک سبز در پایین فولدر ظاهر شود.

قدم سوم:Drop Box را بر روی هر سیستمی‌که می‌خواهید نصب کنید. و با ورود به اکانت خود می‌توانید فولدر Drop Box حاوی فایلهای خود را در کامپیوتر دیگر ببینید و از آنها استفاده کنید.

هر تغییری که بر روی فولدر ایجاد کنید فورا بر روی فولدرها در کامپیوترهای دیگر اعمال می‌شود.

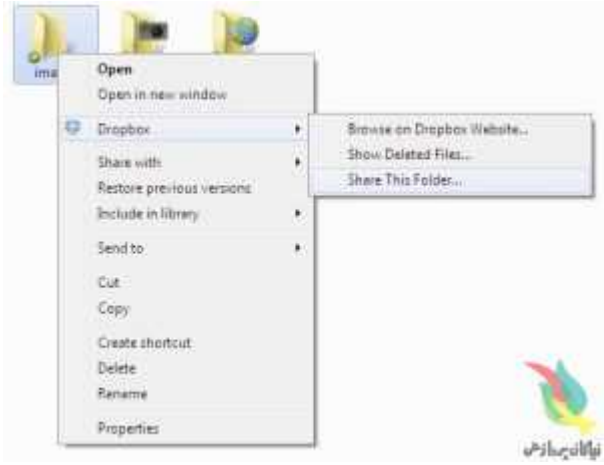
چگونه فولدر خاصی را در اختیار افراد دیگر بگذاریم؟

برای این کار شما دو راه دارید.

اول:استفاده از برنامه تحت ویندوز.

برای اینکه فقط یک فولدر مخصوص را در اختیار فرد مورد نظر قرار دهید کافیست یک فولدر جدید درون فولدر اصلی ایجاد کنید سپس بر روی آن راست کلیک کنید بر روی Drop Box > Share This folder بروید.که شما به سایت منتقل خواهید شد.

در آخر ایمیل فرد مورد نظرتان را وارد کنید و می‌توانید یک متن کوتاه هم بنویسید سپس آن را ارسال کنید.



دوم:از طریق سایت

وارد اکانت خود شوید . محل فولدری را که می‌خواهید مشخص کنید و با زدن Share This Folder آن را به ایمیل مورد نظر به همراه یک پیام دلخواه بفرستید.

پس از ارسال سریعا یک امیل به فرد مقابل به همراه یک دعوت نامه ارسال خواهد شد.

نکاتی هم در این مورد لازم است بدانید.

*شما نمی‌توانید فولدری را که درون **Public Folder** است **share** کنید.

*شما هیچ فولدری که درون یک فولدر **Share** شده باشد را نمی‌توانید **Share** کنید.

*هر کسی که شما به فولدر دعوت کنید می‌توانید فایل اضافه یا حذف کند.

*هرکسی که شما دعوت کرده باشید می‌تواند افراد دیگر را دعوت کند.

*فقط کسی که فولدر را ساخته می‌تواند افراد را از اشتراک حذف کند.

*اگر دو نفر همزمان باهم در فولدر تغییری ایجاد کنند هر دو تغییر انجام می‌شود.برای اطلاع بیشتر از چگونگی این تغییر اینجا را بخوانید.

ویژگی‌هایی که خیلی توجه من را جلب کرد اول از همه سادگی کار و لذت بخش بودن آن بود.

همچنین اینکه فایلهای پاک شده قابل بازگرداندن هستند. همچنین ۲ گیگابایت فضای رایگان در اختیارتان قرار می‌دهد که می‌توانید آن را با پرداخت اشتراک ماهیانه ۵۰ و حتی ۱۰۰ گیگ هم ارتقا دهید.

که البته اگر فقط برای انتقال فایل‌های کاری سبک استفاده کنید ۲ گیگ کافیست.

قابلیت دیگر هم امکان استفاده از **Drop Box** بر روی **iPhone** .و **iPod Touch** و کلا اکثر محصولات **Apple** قابل استفاده است.

همچنین وب سایت **drop Box** بر روی **Black berry** و **android** هم کار می‌کنم.

Browser هایی که **Drop Box** بر روی آنها قابل اجراست.

- +Internet Explorer 7
- +Safari 3
- +Firefox 3
- +Opera 9

سیستم مورد نیاز:

- At least 512MB of RAM
- Free space on your computer equal to your Dropbox storage quota.
- (Windows XP, Windows Vista, and Windows 7 (32 and 64-bit
- Mac: OS X Tiger (10.4) or later

- Ubuntu 7.10+ and Fedora Core 9+.

برای عضویت در Drop Box اینجا کلیک کنید.

سه ویژگی در گوگل کروم که معمولا دیده نمی شود!

۱_ Other Devices
یکی از قدرتمند ترین قابلیت های کروم، توانایی همگام سازی خوب آن است و –نه تنها بوکمارک ها و گذرواژه ها را شامل می شود بلکه- امکان سینک تب های باز را نیز داراست { از Setting => Advanced sync Settings می توانید این قابلیت را اضافه نمائید}.
برای مثال اگر مرورگر کروم بر روی رایانه ها، اسمارت فون ها و یا تبلت های دیگر نصب شده باشد می توانید از یک یک آن ها برای دسترسی به تب های باز روی رایانه مبدا استفاده نمائید؛ ابتدا یک تب جدید را باز و سپس بر روی منوی Other devices موجود در گوشه پائینی آن تب کلیک کنید. اکنون لیستی دسته بندی شده از تب های باز را از تمامی موارد موجود در مروگر کروم را خواهید دید. بسیار دسترس اما غیر قابل تصور!

۲_ Recently Closed

همانطور که شاید بدانید، اگر به صورت تصادفی صفحه ای را ببندید، اگر مایل باشید می توانید سریعاً آن را با فشردن کلید های Ctrl-Shift-T پیدا نموده و اجرا کنید. با این حال، اگر موردی را بخواهید که به تازگی در آن نبوده اید یا حتی از مواردی باشد که در این لیست به دست آمده با استفاده از فشردن این کلید ها موجود نباشد چگونه عمل می کنید؟

چیزی که شما به آن نیاز دارید، لیستی از تمامی تب های بسته شده است که کروم آن را کاملا تحت پوشش خود دارد؛ هنگامی که در گوشه پائینی هستید به گزینه بعدی Other Devices دقت بیشتری کنید، منوی The Recently Closed همانجا قرار دارد. با کلیک بر روی آن ۱۰ تب پایانی بسته شده را مشاهده خواهید کرد.

۳_ Web Store

افرادی که جدیدا به مجموعه کروم می پیوندند، شاید از قابلیتی که گوگل از کتابخانه از برنامه ها به راحتی از وب استور در اختیارشان قرار می دهد آگاه نباشند.

اگر شما هم از دسته افرادی هستید که با آن برخورد نداشته اید، می توانید از همان گوشه درست در گزینه کنار آخرین تب ها بسته شده آن را مشاهده نمائید. سپس اگر بر روی Web Store کلیک کنید، مسیر اپ ها در تبی جدید بازخواهد شد. اکنون می توانید به جستجوی مواردی که برای نصب شدن نیاز دارید بپردازید.

چه ایمیل هایی رو هرگز باز نکنیم ؟

روزانه میلیون ها ایمیل خطرناک و ویروسی در شبکه جهانی رد و بدل می شود و هدف همه آنها یک چیز است. به دردسر انداختن کاربران و بالا کشیدن پول آنها و خالی کردن حساب بانکی‌شان، بخش کوچی از اهداف این نامه‌های الکترونیکی هستند.

البته اکثر ایمیل‌های خطرناک و ویروسی غیر منتظره هستند و معمولا کاربران را در تشخیص دچار سردرگمی می‌کنند. اما چگونه می توان ایمیل های ویروسی و آلوده را از ایمیل های درست و واقعی تشخیص داد؛

ایمیل‌هایی با نام های اشتباهی

در دنیای واقعی آدرس اشخاص با ذکر پلاک منزل و شماره خیابان مشخص می شود. در فضای اینترنت نیز هر کامپیوتری با اعداد منحصر به فردی که بهIPمعروف است معین می‌شود که به وسیله آن راحت تر می توان کاربر را پیدا کرد.

همانند دفتر تلفن که نام هر شخص با شماره مخصوصی تعیین شده و

معین است. اما برای سهولت در کار این شماره هایIPبا یک نام مشخص می‌شود که با وارد کردن آن در مرورگر می‌توان به سایت موردنظر دسترسی پیدا کرد. مسلما بدون اینIPکامپیوتر نمی تواند آدرس را بیابد.در ایمیل های شخصی نیز افراد همزمان از اعداد و حروف استفاده می کنند.

اما گیرنده ایمیل تنها قادر به خواندن آدرس ایمیل هاست و نه خواندن شمارهIPآنها اما هکرها می توانند برنامه ایمیل های شما را طوری تغییر دهند که آدرس ایمیل شما با آدرس ایمیل فرد دیگر یا شرکتی مشهور یکسان شود. فرد گیرنده نیز به محض دریافت این ایمیل گمان می کند که از این فرد یا شرکت مذکور پیغامی دارد. لذا همواره مراقب باشید که حتی ایمیل های افرادی را که می شناسید را نیز با احتیاط باز کنید و قبل از آن از ارسال چنین ایمیلی از طرف آن فرد اطمینان حاصل کنید.

تجارت کثیف با ایجاد وحشت، طمع و جلب اعتماد

در بسیاری از مواقع جنایتکاران با ارسال ایمیل‌هایی با نام مقامات سیاسی و عنوان «احضاریه پلیس» و نامه‌ای که در آن اتهاماتی در خصوص کالاهای تقلبی مطرح شده از دریافت کننده ایمیل درخواست می کنند که با کلیک بر روی لینک ذکر شده از جزئیات اتهام آگاه شوند.کاربری که روی لینک معرفی شده کلیک کند کامپیوتر خود را با بدافزارها آلوده کرده است.همچنین ایمیل های با عناوینی چون «شما برنده شده اید» یا «حساب بانکی تان مسدود شده است» و یا «اخطاریه» نیز حاوی لینک هائی با کدهای اشتباهی و پیوست های آلوده هستند.

برای خوشبینی بیش از اندازه باید بهای سنگینی بپردازید

کاربران هیچگاه نباید به سرعت روی لینک خاصی کلیک کنند و یا پیوست های آن را باز کنند. هر قدر هم عنوان ایمیل وسوسه کننده و وحشت برانگیز باشد زیرا بانک ها، مراجع دولتی و رسمی و شرکت های مطرح هیچگاه از طریق ایمیل اطلاعات حساس همانند رمز کارت اعتباری و یا اطلاعاتی در خصوص حساب بانکی و یا رمز عبور شما را درخواست نمیکنند.

۷ نکته درباره اینترنت که احتمالا نمی‌دانید!

امروزه عادت بر این است که معمولا کاربران دیگر پرسش‌های خود را از کسی نمی‌پرسند، بلکه مستقیم به سراغ گوگل و Bing رفته و از اینترنت پاسخ خود را می‌خواهند؛ اما اگر از ما بپرسند اطلاعات ما از اینترنت چیست، چه باید بگوییم و از اینترنت چقدر می‌دانیم؟

امروزه عادت بر این است که معمولا کاربران دیگر پرسش‌های خود را از کسی نمی‌پرسند، بلکه مستقیم به سراغ گوگل و Bing رفته و از اینترنت پاسخ خود را می‌خواهند؛ اما اگر از ما بپرسند اطلاعات ما از اینترنت چیست، چه باید بگوییم و از اینترنت چقدر می‌دانیم؟ ما در اینجا شما را با هفت نکته جالب درباره اینترنت آشنا می‌سازیم که احتمالا از آنها بی‌خبرید!

برخی از کاربران گمان می‌کنند با استفاده از Private Browsing امنیت حریم خصوصی خود را حفظ می‌کنند. واقعیت این است، در حالی که وب‌گردی در حالت Private در مرورگر هرچند به افزایش ضریب امنیت تا حدی کمک می‌کند، به هیچ وجه شما را نامرئی نمی‌کند! در این حال

هنوز شما قابل رصد و هک شدن هستید و هکرها هنوز هم می‌توانند به سادگی اطلاعات شما را بدزدند.

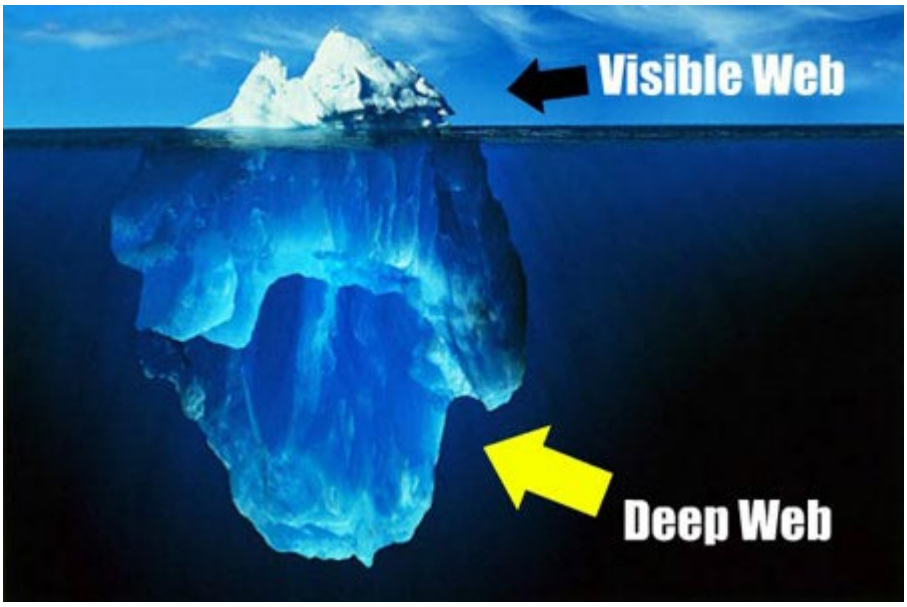
در حالی که هر روزه از اینترنت به عنوان یکی از ابزارهای اصلی برای ارتباطات و حتی و کسب و کار خود بهره می‌بریم، باید یک بار از خود بپرسیم چقدر از اینترنت می‌دانیم. اینکه اینترنت بواقع چیست و چگونه می‌توان از آن بهره برد؟!

شاید به اندازه‌ای در فضای وب و سایبری مشغول و غرق شده‌ایم که اساسا فراموش کرده‌ایم در چنین فضایی هستیم؛ اما لازم است گاهی سری بالا کنیم و از ماهیت آنچه در آنیم و تاریخچه آن بیشتر آگاهی به دست آوریم.

البته در اینجا ما نمی‌خواهیم وارد مبحث ماهیت اینترنت و وب و یا تاریخچه آن شویم، چرا که این موضوع مباحث مفصل و چالشی در بر دارد و قطعا تعریف ماهیت اینترنت چیزی نیست که در یک گزارش کوتاه بتوان جامع به آن پرداخت، بلکه هدف ما در اینجا این است که شما را با هفت نکته جالب در خصوص اینترنت و وب آشنا سازیم که در آن ضمن تمرکز بر جنبه سرگرم‌کننده، کمی چاشنی اطلاعات عمومی در خصوص اینترنت نیز مخلوط است.

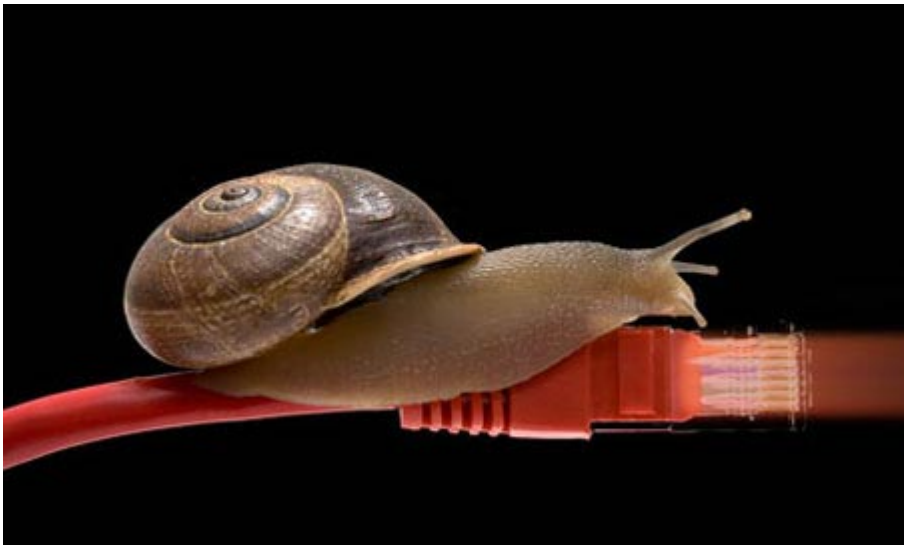
۱ ـ انسان ها تنها ۴۹ درصد از کل ترافیک اینترنت را شکل داده‌اند. الباقی ۵۱ درصد ترافیک اینترنت توسط Bot ها (ربات‌های رایانه‌ای که در واقع برنامه‌هایی برای انجام امور تعریف شده به شکل خودکار هستند) شکل داده شده است.

۲ ـ مجموع وب‌سایت‌های نامرئی و ثبت نشده که در موتورهای جستجو یافته نمی‌شوند (Deep Web) پانصد برابر بزرگتر و بیشتر از وب‌سایت‌های مرئی و قابل جستجو و بازدید (Surface Web) است.



۳ ـ سرعت اینترنت در پایگاه بین‌المللی فضایی بیشتر از متوسط سرعت اینترنت در استرالیاست و متوسط سرعت اینترنت در استرالیا، بیش از سه و نیم برابر متوسط سرعت اینترنت در ایران است.

۴ ـ هنگ کنگ با متوسط سرعت اینترنت ۸۲.۶ Mbps سریع‌ترین اینترنت دنیا و نیجر با ۰.۶ Mbps تنبل‌ترین اینترنت دنیا را دارند. ایران با متوسط سرعت ۴.۰۲ Mbps در رتبه ۱۵۴ در بین ۱۹۲ کشور قرار گرفته است.



۵- چهار تا پنج سال طول کشید تا رقم کاربران اینترنت به پنجاه میلیون رسید. در حالی که برای رسیدن تلویزیون به همین میزان کاربر، سیزده سال و برای رادیو، هجده سال زمان صرف شد.

۶ – نخستین وب‌سایت دنیا در سال ۱۹۹۱ ساخته شد. شما می‌توانید این وب‌سایت را در (www.info.cern.ch) ببینید.

۷ – نخستین وب‌کم در دانشگاه کمبریج و در سال ۱۹۹۳ برای رصد و دیدن یک قهوه جوش مورد استفاده قرار گرفت.

منبع:http://www.ostovarit.com/single/article/2384/7%20نکته%۲۰د رباره%۲۰اینترنت%۲۰که%۲۰احتمالا%۲۰نمی‌دانید!

فضای ابری چه کاربردی دارد؟

به گزارش ایتنا از مرکز ماهر، داریوش زندی اظهار کرد: تعداد کثیری از شرکت‌های مختلف به این فضای ابری علاقه نشان داده‌اند و مقدار محدودی از این فضا را در اختیار کاربران به صورت رایگان قرار می‌دهند.

وی افزود: این فضا دقیقاً شبیه هارد درایو شما روی سیستم است منتها برای دسترسی به آن باید از اینترنت استفاده کنید در ضمن این فضا بر روی هارد درایو شما قرار ندارد و بر روی سرورهای قدرتمندی در کشورهای توسعه‌یافته قرار دارد.

این کارشناس ارشد هوش مصنوعی بیان کرد: برای دسترسی به این فضا هر کاربری نیاز به یک حساب کاربری دارد. کاربر با وارد شدن به حساب کاربری خود در هر مکانی و روی هر سیستمی می‌تواند به فضای ابری خود دسترسی داشته باشد.

وی عنوان کرد: از مهم‌ترین شرکت‌هایی که در این حوزه فعالیت دارد دراپ باکس۱ است. با وارد شدن به سایت دراپ باکس و ساخت یک حساب کاربری در آن از دو گیگابایت فضای مجانی آن استفاده کنید. اگر به فضای بیشتری نیاز داشته باشید باید در عوض پولی بپردازید که برای کاربران ایرانی مشکلاتی را به همراه دارد.

وی اعلام کرد: مزیت دارپ باکس وجود نرم‌افزار لازم در تمام سیستم‌عامل‌های موجود و همچنین داشتن اپلیکیشن موبایل نیز است.

زندی تصریح کرد: از این به بعد اگر می‌خواهید به اطلاعاتتان در هرجایی و بر روی هر کامپیوتری و حتی روی گوشی‌تان دسترسی داشته باشید با ساخت یک اکانت در دراپ باکس از این امکان لذت ببرید.

وی ادامه داد: فرض کنید روی یک فایل متنی در منزل در حال کار هستید، شما می‌توانید آن را در فضای ابری خود قرار دهید و در محل

کار آن را ویرایش کنید در واقع می‌توانید روی لپ‌تاپتان یک سند خلق کنید و آن را روی تلفن همراهتان ببینید و حتی بعداً روی سیستم‌تان در محل کار آن را ویرایش کنید.

این کارشناس ارشد هوش مصنوعی خاطرنشان کرد: همچنین در دراپ باکس این امکان مهیا شده است که می‌توانید به یک فایل خاص در فضای ابری خودتان لینک بدهید و آن را با دیگران به اشتراک بگذارید.

منبع:http://www.ostovarit.com/single/article/2561/فضای%۲۰ابری%۲۰چه%۲۰کاربردی%۲۰دارد؟

چگونه ایمیل اسپم را متوقف کنیم؟

این مقاله به شما مختصرا در مورد نحوه متوقف کردن ایمیل های اسپم توضیح می دهد. ایمیل های اسپم (هرزنامه) نه تنها مقدار قابل توجهی از فضای جهان مجازی را به خود اختصاص داده اند ، همچنین می توانند وسیله ای برای سرقت های امنیتی باشند. برای اطلاعات بیشتر در مورد تهدیدات ناشی از ایمیل های اسپم ، لطفا این مقاله را مطالعه نمایید.

آیا می دانیددر کشورهای پیشرفته فردی که ایمیل اسپم(هرزنامه) برای شما ارسال می کند مجرم بوده و علاوه بر بلوک شدن وب سایتش باید جریمه نقدی زیادی هم برای هر ایمیلی که برای شما می فرستد پرداخت نماید ؟

ما در این مقاله قصد داریم برخی از روش های موثر در مورد چگونگی متوقف کردن ایمیل های اسپم را به شما ارائه دهیم.

چرا ایمیل های اسپم یک تهدید به حساب می آیند؟

ایمیل های اسپم گاها ممکن است ابزار خوبی برای سرقت هویت شما توسط هکرها باشند.شما با کلیک بر روی لینک موجود در این گونه ایمیل ها ، ممکن است به طور ناخواسته برای فرستنده ی ایمیل ، این امکان را فراهم کنید که به بسیاری از اطلاعات مهم موجود در کامپیوتر شما دسترسی پیدا کند.مانند شماره Social Security،پسورد، مشخصات حساب و فایل های شخصی و غیره ، یعنی همه ی اطلاعات محرمانه ای که از آن ها استفاده می نمایید ،با استفاده از این روش تمام اطلاعات شما توسط فرد دیگری که این ایمیل را برایتان فرستاده است سرقت (سرقت هویت)می شود.

مشکل دیگر این ایمیل های اسپم این است که بعضا حاوی نرم افزارهای مخرب ،نرم افزارها جاسوس و غیره می باشند.

شما تنها با یک کلیک ساده روی هر یک از لینک ها ی ایمیل اسپم ممکن است دانلود برخی از نرم افزارهای مخرب را در کامپیوتر خود آغاز نمایید.

بنابراین شما باید اطلاعات بیشتری در مورد حفاظت ازسیستم تان در مقابل ابزارهای تبلیغاتی مزاحم و نرم افزارهای جاسوسی بدست آورید. با استفاده از این اطلاعات، ما به شما می گوییم که در مورد این واقعیت کاملا مطمئن باشیدکه بسیاری از ایمیل های اسپم تهدیدی برای حریم خصوصی شما می باشند.

چگونه ایمیل های ناخواسته را متوقف کنیم ؟

بسیاری از ارائه دهندگان سرویس ایمیل(یاهو ،گوگل و …) تا حد زیادی اقدامات لازم برای مسدود کردن ایمیل های اسپم را می دانند. بله ، شما باید متوجه پوشه اسپم ،در حساب ایمیل خود باشید. جایی که بسیاری از ایمیل های اسپم به صورت خودکار به آنجا منحرف می شوند. اما باز هم شما برخی از ایمیل های اسپم را در حساب اصلی خود دریافت می نمایید. شما می توانید اقدامات زیر را انجام دهیدکه می تواند به شما در متوقف کردن ایمیل های اسپم کمک کند.

هرگز پاسخ ایمیل اسپم را ندهید

مسلما شما آن قدر باهوش هستید که هرگز به یک ایمیل اسپم پاسخ ندهید و یا روی لینک موجود در این ایمیل های ناخواسته کلیک نکنید . من به شخصه هیچ عنوان بر روی ایمیل های ناشناس کلیک نمی کنم و به سرعت آنها را Delete خواهم کرد . اما با این حال ممکن است گاهی تحت شرایطی ، این کار را انجام دهید مانند پاسخ دادن به یک ایمیل اسپم احساسی یاجواب دادن به یک سوال در ایمیل هرزنامه ای که برایتان ارسال شده است. کلیک روی ایمیل های اسپم تنها راهی است که شما به کسی که ایمیل اسپم رابرایتان ارسال کرده اجازه می دهید به سیستم تان نفوذ کند ، باید بدانید که این ایمیل ها همیشه فعال هستند. فرستندگان ایمیل اسپم همیشه حواسشان هست که آدرس ایمیلی فعال باشد تا او را طعمه قرار دهند.

مورددیگر اینکه گاهی حتی با کلیک کردن بر روی یک دکمه مانند قبول’اشتراک’ در ایمیل نیز راه برای فرستنده ایمیل اسپم باز خواهد شد تا شما را پیدا کند و بداند که آدرس ایمیل شما فعال است. پس تحت هیچ شرایطی روی ایمیل های ناشناس و مشکوک کلیک نکنید تا فرستنده ایمیل اسپم، ایمیل شما را غیر فعال تلقی نماید.

استفاده از ایمیل های مختلف برای شناسه ها

با استفاده از آدرس های ایمیل مختلف ، برای مقاصد مختلف، ایده ی هوشمندانه ای است. اگر شما کسی هستید که استفاده ازسیستم خرید آنلاین را دوست دارید ، استفاده از یک آدرس ایمیل دیگربرای همه معاملاتی که از طریق اینترنت انجام میدهید روش خوبی خواهد بود. یعنی آدرس ایمیلی راکه برای کسب و کار و یا استفاده شخصی تان استفاده می کنید ، برای انجام معاملات اینترنتی مورد استفاده قرار ندهید. در این شرایط شما می توانید هر زمان که خرید آنلاین انجام میدهید، بدون نگرانی آدرس پست الکترونیکی خود را به فروشنده بدهید.

استفاده از فیلترهای هرزنامه

استفاده از فیلترهای اسپم ارائه شده توسط ارائه دهندگان خدمات پست الکترونیکی ، یکی دیگر از راه های موثر برای کاهش دریافت ایمیل های اسپم هستند. اگر چه این فیلترهای هرزنامه به طور خودکار حذف می شوند و گاهی باز هم برخی از این گونه ایمیل های اسپم را دریافت می کنید ، ولی شما می توانید ابتکار عمل به خرج داده و با مارک کردن این گونه ایمیل ها کاری کنید که بازهم این گونه ایمیل ها به عنوان اسپم به صندوق پستی بروند. کافی است که ایمیل خاصی را انتخاب کنید و آن را به عنوان اسپم علامت گذاری نمایید. به این روش شما می توانید دریافت ایمیل های اسپم را فیلتر نمایید.

این ها اطلاعات کمی در مورد نحوه متوقف کردن ایمیل های اسپم بود.

در ایالات متحده آمریکا قانونCAN – SPAM وجود دارد ، این قانون چیزی است که حاکم بر تمام دادرسی هایی مربوط به سازمان های اسپم است. به امید روزی که در کشور ما نیز این قانون جزئی از قوانین حاکم بر این صنعت شود هر چند با توجه به رشد روز افزون تجارت آنلاین در ایران این روز زیاد دیر نیست.

منبع:-http://www.amoozesh-computer.ir/computer-traning-pro/how-to-stop-email-spam