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 کا ر

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.

نت تاپ چیست؟

یک رایانه درابعاد کوچک است حدود ~, 25(H)mm x 135(D) x W) 450g) که تمامی قابلیتهای یک رایانه را درخود جای می دهد و به عنوان رقیب اصلی رایانه های رومیزی معمولی می باشد.علت نامگذاری این رایانه به این نام این است که NetTop از دو کلمه نت (Internet) و تاپ (Desktop) به معنای میزکار تشکیل شده است.

درمقایسه با رایانه های معمولی نت تاپ ها نه تنها کوچکتر ارزانتر

و سبکترند بلکه مصرف برق به مراتب کمتری هم دارند. یک نت تاپ در حدود ۲۳ وات برق مصرف می کند.

نت تاپ را میتوان در پشت مانیتورهایتان نصب کنید که به نسبت کیس های بزرگ امروزی فضای کمتری را اشغال می کند البته میتوان آنها را با استفاده از پایه روی میز قرارداد.

NetTop ها از لحاظ سیستم خنک کننده به دو بخش عمده دسته بندی می شوند. دسته اول در قسمت تهویه خود دارای فن و دسته دوم که فاقد فن هستند ازفناوری هوای خنک استفاده می کنند ، این قابلیت باعث شده که NetTop به عنوان یکی از کم صداترین تجهیزات فن آوری اطلاعات در منازل و دفاتر کار و شرکت ها مطرح شوند.

البته لازم به ذکر است که طراحی نت تاپ ها به گونه ای است که بیشتر بر روی دستیابی های مبتنی بر وب تمرکز دارند تا انجام فعالیت های محاسباتی پیشرفته،بنابراین معمولا نسبت به کامپیوترهای شخصی همتای خود دارای قدرت پردازش و حافظه کمتری می باشند که این باعث اجرانشدن سریع و دقیق می شود.

همچنین با وجود اینکه کامپیوترهای امروزی کمتر بر روی رسانه های نوری مانند سی دی و دی وی دی جهت ذخیره سازی تمرکز دارند اما به طور کامل نمی توان آنها را نادیده گرفت و این در حالیست که بیشتر نت تاپ ها فاقد سی دی /دی وی دی رام می باشند.

اجزا و ویژگی های یک نت تاپ:

– قابلیت نصب سیستم عامل های ویندوزو لینوکس را دارا می باشند.

– کارت شبکه مینیاتوری GB LAN و Wi-Fi IEEE 802.11b/g/n
– درگاه های HDMI , USB 3.0
– کارت خوان داخلی SD/SDHC/MS/MS Pro/MMC
– درگاه های USB 2.0, DVI ،صدا و میکروفون
– استفاده از از هاردهای ۵٫۲ اینچی یا SSD و حافظه DDR3

Nettop ها را می توان بر اساس توان آنها در ادارات ، بانک ها ، مدارس ، شرکت های خصوصی ، کارخانجات و در خانه مورد استفاده قرار داد.

به منظور آشنایی بیشتر با مدل های ارائه شده نت تاپ ها در زیر چندین نمونه از آنها را معرفی خواهیم کرد.

– نت تاپ سولمیت آمیس (Solmate AMIS Nettop)
* پشتیبانی از DOS – XP – VISTA – SEVEN – LINUX
* پردازنده Intel Atom D525 1.8 Dual Core با تکنولوژی CUDA چهار هسته پردازشی
* گرافیک NVidia ION2 Geforce 9400 M 512 DDR3
۴/۲ * گیگ رم DDR3 ، هارد ۳۲۰ گیگ پشتیبانی تا ۵۰۰ گیگ
* ۴ عدد پورت USB ، شبکه ۱ گیگ و شبکه وایرلس سری N ، خروجی گرافیک VGA و HDMI ، ورودی و خروجی صدا

– نت تاپ سولمیت جنریک (Solmate Generic Nettop)
* پشتیبانی از DOS – XP – LINUX
* پردازنده Intel Atom D510 1.66 Doul Core
* گرافیک Intel GMA 3150 256
۲ * گیگ رم DDR|| ، هارد ۲۵۰ گیگ پشتیبانی تا ۵۰۰ گیگ
* ۶ عدد پورت USB ، شبکه ۱ گیگ ، خروجی گرافیک VGA ، ورودی و خروجی صدا
* کاملا بی صدا ، ۰٫۵ لیتر حجم ، ۶۵۰ گرم وزن ، ۱۸ وات میانگین مصرف برق ، قابلیت اتصال پشت مانیتور

– نت تاپ مکس دیتا
*پشتیبانی از DOS – XP – VISTA – SEVEN – LINUX
*پردازنده Intel Atom 330 1.6 Dual Core با تکنولوژی CUDA چهار هسته پردازشی
* گرافیک NVidia ION Geforce 9400 M 512
۲ * گیگ DDR|| ، هارد ۲۵۰ گیگ پشتیبانی تا ۵۰۰ گیگ

* ۴ عدد پورت USB ، شبکه ۱ گیگ ، خروجی همزمان گرافیک DVI و HDMI ، ورودی و خروجی صدا
* Card Reader ،WLan 802 .11 b/g/n
* کاملا بی صدا ، ۰٫۵ لیتر حجم ، ۵۵۰ گرم وزن ، ۱۸ وات میانگین مصرف برق ، قابلیت اتصال پشت مانیتور

– نت تاپ سولمیت مدیا (Solmate Media Nettop)
* پشتیبانی از DOS – XP – VISTA – SEVEN – LINUX
* پردازنده Intel Atom 330 1.6 Dual Core با تکنولوژی CUDA چهار هسته پردازشی
* گرافیک NVidia ION Geforce 9400 M 512
۲ * گیگ / ۴ گیگ رم DDR|| ، هارد ۲۵۰ گیگ پشتیبانی تا ۵۰۰ گیگ
* ۵ عدد پورت USB ، شبکه ۱ گیگ ، خروجی گرافیک DVI ، ورودی و خروجی صدا
* Card Reader ،e-sata ،Infra Red ،WLan 802 .11 b/g
* کاملا بی صدا ، ۰٫۷ لیتر حجم ، ۸۵۰ گرم وزن ، ۱۸ وات میانگین مصرف برق ، قابلیت اتصال پشت مانیتور

– نت تاپ سولمیت تاور
* پشتیبانی از DOS – XP – VISTA – SEVEN – LINUX
* پردازنده Intel Atom 330 1.6 Dual Core با تکنولوژی CUDA چهار هسته پردازشی
* گرافیک NVidia ION Geforce 9400 M 512
۳ * گیگ رم DDR|| ، هارد ۲۵۰ گیگ پشتیبانی تا ۵۰۰ گیگ
* ۶ عدد پورت USB ، شبکه ۱ گیگ ، خروجی گرافیک DVI ، ورودی و خروجی صدا
* کاملا بی صدا ، ۰٫۵ لیتر حجم ، ۶۵۰ گرم وزن ، ۱۸ وات میانگین مصرف برق ، قابلیت اتصال پشت مانیتور

تروجان چیست؟ و چگونه در مقابل آن ایمن شویم؟

در این مطلب قصد داریم راجع به شاخه ای از بدافزارها به نام «اسب تروجان» که به اختصار «تروجان» نامیده می شوند صحبت کنیم. تروجان ها بر خلاف ویروس ها، کرم ها و … توانایی تکثیر خود را ندارند. آنها بسیار شبیه نرم افزارهای مفید و کاربردی رفتار می کنند، اما در درون خود کدهای مخفی دارند که باعث دسترسی هکر سازنده تروجان به کامپیوتر هدف (کامپیوتر آلوده شده) و به دست گرفتن کنترل آن می شوند.

علت نام گذاری

نام این بدافزارها به ماجرای تسخیر تروا توسط یونان برمی گردد، که با ساختن یک اسب چوبی و مخفی شدن درون شکم آن به شهر تروا نفوذ کرده و آن را به تصرف خود درآوردند. در این داستان اسب تروا نقش یک بدافزار را دارد و شهر تروا مانند کامپیوتر کاربری است که توسط اسب تروا آلوده می شود. به همین دلیل بعضی بکار بردن کلمه «تروجان» برای بدافزار را اشتباه و کلمه «اسب تروجان» را صحیح می دانند.

مقدمه

تروجان ها بر خلاف ویروس ها، کرم ها و … توانایی تکثیر خود را ندارند. آنها بسیار شبیه نرم افزارهای مفید و کاربردی رفتار می کنند، اما در درون خود کدهای مخفی دارند که باعث دسترسی هکر سازنده تروجان به کامپیوتر هدف (کامپیوتر آلوده شده) و به دست گرفتن کنترل آن می شوند. البته در مواردی که چند کاربر از یک کامپیوتر استفاده می کنند سطح دسترسی هکر بسته به سطح دسترسی کاربر آلوده و نوع تروجان تفاوت می کند.

اهداف و عملکرد

زمانی که هکر به کامپیوتر هدف نفوذ می کند، احتمالاً قصد انجام این اعمال را در کامپیوتر هدف داشته باشد:

استفاده از کامپیوتر به عنوان یک ابزار برای نفوذ به دیگر سیستم‌ها و شبکه ها

دزدیدن اطلاعات (مثل رمزهای عبور)

نصب نرم افزارها (مثلا یک بدافزار)

دانلود و آپلود فایل‌ها و استفاده از پهنای باند

تغییر یا حذف فایل ها

Key Logging (ثبت فعالیت هایی که کاربر انجام می دهد. برای مثال یک Key Logger می تواند تمام دکمه های صفحه کلید را که فشار می

دهید به ترتیب ثبت کند و آنها را به هکر سازنده اش ارسال کند.)
دیدن صفحه نمایش کامپیوتر هدف
پر کردن فضای خالی کامپیوتر هدف

تروجان برای انجام اهداف خود نیاز به ارتباط با هکر سازنده اش دارد. البته این گونه نیست که هکر برای هر کدام از تروجان های خود دستور خاصی بدهد، بلکه می‌تواند در اینترنت جستجو کرده و کامپیوترهای آلوده را پیدا کند. سپس کنترل هر کدام را که بخواهد به دست می گیرد.

انتقال و نصب

تروجان به روش‌های زیر کامپیوتر را آلوده می کند:
۱-دانلود نرم افزارها (تروجان قسمتی از نرم افزاری است که کاربر آن را از اینترنت دانلود و نصب می کند.)
۲-سایت های دارای کدهای مخرب (مثلا زمانی که وارد یک سایت می شوید، سایت یک برنامه روی کامپیوتر اجرا می کند و تروجان را روی کامپیوتر کپی می کند.)
۳-فایل‌های ضمیمه ایمیل (Email attachments ممکن است همراه یک ایمیل فایلی باشد که اگر آن را باز کنید، تروجان منتقل شود.)
۴-استفاده از نقص های نرم افزارها (تروجان از طریق ایرادهایی که در نرم افزارهایی مثل مرورگرهای اینترنتی، مدیا پلیرها و مسنجرها وجود دارد، به کامپیوتر کاربر نفوذ می کند.)

در زیر **راه های مقابله** با موارد بالا را به ترتیب می آوریم:

۱- دانلود نرم افزارها نرم افزارهای اینترنتی به دو گروه کلی

تقسیم می شوند: رایگان و پولی. زمانی که می خواهید از یک نرم افزار رایگان استفاده کنید، حتما آن را از سایت اصلی اش دانلود کنید. اگر آدرس سایت اصلی را نمی دانید، نام نرم افزار را در گوگل – یا هر موتور جستجوی دیگر – جستجو کنید و سایتی که در بالای نتایج می آید را برای دانلود برگزینید. البته معمولا آدرس آن سایت شباهت زیادی به نام نرم افزار دارد. مثلا برای دانلود آنتی ویروس «اوست» به سایت «avast.com» مراجعه کنید. ماجرا درباره نرم افزارهای پولی پیچیده تر است.

برای خرید اینترنتی این نرم افزارها به کارت اعتباری و یک حساب بانکی بین المللی نیاز است که در دسترس همگان نیست. خب برای رفع این مشکل باید نسخه کرک شده (قفل شکسته) نرم افزار را پیدا کنیم و یا به جای نرم افزار پولی از یک نرم افزار مشابه و رایگان استفاده کنیم. ما توصیه می کنیم حتی الامکان از نرم افزار جایگزین و رایگان استفاده کنید، اما برای بعضی نرم افزارها – مثل Photoshop – جایگزین مناسبی وجود ندارد و کاربران مجبور به استفاده از نسخه های کرک شده هستند.

همان طور که می دانید این کار خلاف قانون کپی رایت بوده و دقیقا از همین جا است که خطرات آغاز می شود. بسیاری از نرم افزارهای کرک شده حاوی انواع بدافزارها خصوصا تروجان هستند. این امر کاملا طبیعی است. شما خودتان را جای یک هکر بگذارید. آیا حاضرید برای رضای خدا مدت ها وقت و انرژی خود را بگذارید تا بتوانید یک نرم افزار را کرک کنید و آن را به رایگان در اختیار دیگران قرار دهید؟ مسلما نه.

[illegible]

خب پس تکلیف چیست؟ توصیه ما این است که حتی الامکان از نرم افزارهای کرک شده استفاده نکنید و اگر مجبور بودید، قبل از اینکه نرم افزار را نصب کنید، پوشه حاوی نرم افزار را با آنتی ویروس و دیگر نرم افزارهای امنیتی خود کنترل (scan) کنید. سپس نرم افزار را نصب کرده و این بار کل کامپیوتر خود را اسکن کنید. اگر در

اسکن چیزی پیدا نشد که خوش به حال تان و می توانید دفعات بعد هم از همین نسخه کرک شده استفاده کنید. ولی اگر در اسکن بدافزاری پیدا شد، ضمن آنکه به آنتی ویروس می گویید که آن بدافزار را پاک کند، توصیه می شود دفعات بعد از نسخه دیگری استفاده کنید. البته اگر نرم افزارهای امنیتی شما قوی و آپدیت (به روز) باشند احتمالا خطر زیادی شما را تهدید نمی کند. یادآوری: یکی از معمول ترین فایل های آلوده به بدافزارها کی جن (Keygen) ها هستند. کی جن ها همان نرم افزارهایی هستند که برایتان رمزعبور تولید (Generate) می کنند.

۲- سایت های حاوی کدهای مخرب
خطر آلودگی از این طریق بستگی مستقیمی به عادات وبگردی تان دارد. اگر شما همیشه به یکسری سایت های شناخته شده و معتبر سر بزنید، خطر زیادی تهدیدتان نمی کند. مشکل زمانی پیش می آید که به دنبال چیزی در موتورهای جستجو می گردید. در این موارد موتور جستجو سایت هایی پیشنهاد می دهد که هیچ شناختی از آنها ندارید و ممکن است حاوی کدهای مخرب باشند.
توصیه هایی برای وبگردی امن تر:
از مرورگر فایرفاکس استفاده کنید.

اگر سرعت اینترنت خوبی دارید از حالت «گشت و گذار محرمانه» استفاده کنید. برای فعال کردن این حالت در فایرفاکس در منوی Tools روی گزینه Private Browsing Windows کلیک کنید. در پنجره بعد روی دکمه Start Private Browsing کلیک کنید. با این کار تمام Tab های فعلی فایرفاکس تان بسته می شوند و پنجره Private Browsing باز می شود. پس از گشت و گذار در اینترنت زمانی که پنجره را می بندید، تمام تاریخچه، کوکی ها و هر فایل دیگری که در زمان وبگردی محرمانه ذخیره شده است، پاک می شوند و در آخر Tab های فایرفاکس عادی تان باز می گردند.

استفاده از افزونه Noscript در فایر فاکس.

۳- ضمیمه هایی که به ایمیل ها الصاق می شوند

هیچ گاه ایمیلی که فرستنده آن را نمی شناسید باز نکنید. بلکه با خیال راحت آن را حذف کنید. اگر از جی‌میل استفاده می کنید آن ایمیل را تیک زده و روی دکمه Report Spam کلیک کنید، تا دیگر ایمیلی از این شخص برای تان نیاید.

نکته: نام فرستنده این ایمیل ها معمولا نام یک بانک معتبر است و در Subject ایمیل نوشته که شما پول فراوانی برنده شده اید و یا از یک نام زیبای زنانه استفاده شده.

۴- استفاده از نقص های نرم افزاری
برای حل این مشکل سعی کنید همیشه نرم افزارهایتان را به روز نگه دارید. خصوصا به روز رسانی های امنیتی (Security Updates) را حتما نصب کنید.

اگر به تروجان آلوده شدید
نرم افزارهای آنتی ویروس توانایی پاک کردن تروجان ها را دارند. آنها حتی می توانند قبل از نفوذ تروجان به سیستم جلوی آن را بگیرند. البته اگر از عملکرد یک تروجان آگاهی کافی داشته باشید، حتی خودتان می توانید آن را پیدا کرده و پاک کنید. البته در مورد تروجان هایی که دسترسی هکر را به سیستم فراهم می آورند، ماجرا کمی پیچیده تر است. در این موارد اگر امنیت کامپیوتر اهمیت زیادی دارد، توصیه می شود کل هارد کامپیوتر را فرمت (پاک) کنید و از ابتدا روی آن سیستم عامل و نرم افزارهای مورد نیاز را نصب کنید.

و در آخر شیوع تروجان ها

با توجه به علاقه روز افزون هکرها به مبحث کنترل کامپیوتر از راه دور، شیوع تروجان در میان بدافزارها در حال افزایش است. طبق آمار مختلف در سه ماهه آخر سال ۲۰۰۹ بین ۷۰ تا ۸۰ درصد از بدافزارهای کشف شده در سراسر دنیا تروجان بودند و این میزان در حال افزایش است. پس بهتر است آنها را جدی بگیرید.

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 می توانید این قابلیت را اضافه نمائید sync Settings}.

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.

پس از هک شدن حساب های شخصی چه باید کرد؟

بسیاری تصور می کنند هک سیستم های رایانه ای و سرقت اطلاعات تنها به شرکت ها و سرویس های بزرگ محدود می شود و اشخاص حقیقی نیاز مبرمی برای حفاظت از رایانه یا دستگاه های دیجتالی خود در مقابله با نفوذ هکرها احساس نمی کنند اما باید گفت در مواردی اشخاص حقیقی نسبت به شرکت های بزرگ، از هک سیستم های رایانه ای و حساب های خود آسیب بیشتری می بینند.

وجود یک حفره امنیتی در نرم افزارهای نصب شده روی رایانه یا تلفن همراه، وجود برنامه های Keylogger و انواع و اقسام روش های دیگر می تواند به نفوذ هکرها به حریم خصوصی کاربران و به خطر افتادن تمامی حساب های شخصی از جمله حساب های بانکی منتهی شود.

با رعایت تمام اصول امنیتی، احتمال نفوذ هکرها کمتر خواهد شد اما هرگز از بین نمی رود. از سوی دیگر، پروسه حفاظت از حساب های شخصی تنها به کاربران محدود نمی شود و تا به امروز بارها خبرهایی از افشا شدن اطلاعات و کلمه های عبور کاربران سرویس های بزرگ با هک شدن سرورهای آنها شنیده ایم. با این وجود در صورت هک شدن حساب های شخصی چه باید کرد و راه های جلوگیری از تبعات آن چیست؟

واکنش سریع با استفاده از پست الکترونیکی

اگر برخی از حساب های اینترنتی شما هک شده و با تغییر کلمه عبور توسط هکر، امکان ورود به آنها وجود ندارد، امید خود را از دست ندهید؛ زیرا در صورت واکنش سریع احتمال بازگرداندن حساب های از دست رفته همچنان وجود دارد.

در هنگام ثبت نام در سرویس های اینترنتی، آدرس پست الکترونیکی خود را ثبت کرده اید و در صورتی که این آدرس از دسترس هکرها در آمان مانده باشد، می توان از آن برای بازگرداندن کلمه عبور استفاده کرد.

این اقدام نخستین گام در مقابله با نفوذ هکرها و بازیابی حساب های از دست رفته محسوب شده و توصیه می شود هر چه زودتر به استفاده از آن اقدام کنید.

در زمان ثبت نام سرویس های ایمیل نیز از شما درخواست می شود به شکل دلخواه آدرس دیگری را به عنوان پست الکترونیکی پشتیبانی معرفی کنید. همواره از این پیشنهاد برای مقابله با هک شدن ایمیل خود و بازیابی کلمه عبور در آینده، بهره بگیرید.

اسکن کامل رایانه

دومین گام، جلوگیری از دسترسی های بعدی و نفوذ مجدد هکرها به اطلاعات شخصی خواهد بود که برای انجام این کار ابتدا باید حرفه امنیتی یا راه نفوذ هکرها را پیدا کنید. برای انجام این کار باید از یک نرم افزار آنتی ویروس و ضد بدافزار برای اسکن کامل رایانه یا تلفن همراه استفاده کنید.

در این مرحله باید از ضد بدافزار و آنتی ویروس هایی کمک بگیرید که مورد تایید کارشناسان بوده و از اعتبار و قدرت کافی در زمینه کاری خود برخوردار باشند. ورود یک تروجان یا نصب Keylogger روی رایانه می تواند به ثبت اطلاعات ورودی و ارسال آنها به هکرها منجر شود و آنتی ویروس های قدرتمند قادر به تشخیص بدافزارها و حذف آنها خواهند بود.

اطلاع از مسیر بدافزارها و ویروس های پیدا شده می تواند به یافتن ریشه آلودگی و رفع آن نیز کمک کند. یک فایل دانلود شده، داده های آپلود شده توسط سایت یا نرم افزارهای بی نام و نشان، همه به نوبه خود می توانند منشأ آلودگی و راه نفوذ هکرها باشند.

نفوذ هکرها به منبع اطلاعات

همان طور که گفته شد، نفوذ هکرها به حساب های شخصی افراد تنها به بی احتیاطی اشخاص حقیقی و کاربران اینترنت مربوط نمی شود. در مواردی هکرها به سرورهای سرویس های بزرگ نظیر یاهو یا جی میل نفوذ می کنند و حجم انبوهی از اطلاعات محرمانه و شخصی افراد را به سرقت می برند.

حتی اگر تمام نکات امنیتی را رعایت کنید، ممکن است سرویس مورد استفاده شما در ابعاد بزرگ مورد دستبرد هکرها قرار بگیرد و در این حالت هیچ کاری از دست کاربران معمولی برنخواهد آمد. برای اطلاع از این گونه اتفاقات باید روی اینترنت نام سرویس خود را با عبارت Password Leak جستجو کنید و با پیگیری اخبار مرتبط مطلع شوید آیا واقعا سرویس مورد استفاده شما با سرقت اطلاعات محرمانه توسط هکرها مواجه شده است یا خیر.

برای نمونه در جولای سال ۲۰۱۲ سرویس پست الکترونیکی یاهو، هک و میلیون ها کلمه عبور کاربران این سرویس جهانی در فضای اینترنت پخش شد. با این اتفاق سایر حساب های افراد مانند حساب فیس بوک یا توییتر آنها نیز با خطر مواجه شد و مقابله با این مشکل کاملا خارج از قدرت کاربران بود.

اوضاع زمانی بدتر می شود که از یک کلمه عبور یکسان برای تمامی حساب های خود استفاده کرده باشید و با فاش شدن آن، تمامی حساب

های تان به راحتی در دسترس هکرها قرار بگیرند.
برای مقابله با این مشکل توصیه می شود از کلمه های عبور مختلف برای حساب های اینترنتی متفاوت خود بهره بگیرید و به منظور مقابله با فراموش کردن آنها از برنامه های مدیریت کلمه عبور استفاده کنید.
منبع: هفته نامه عصر ارتباط

تفاوت بین روش‌های رمزنگاری WEP، WPA و WPA2 در شبکه‌های بی سیم

امروزه با گسترش استفاده از اینترنت برای انجام فعالیت‌های خانگی و اداری و همچنین گسترش نفوذ تلفن‌های هوشمند در میان کاربران، مودم‌های بی سیم جز جدایی ناپذیر بسیاری از منازل و دفاتر در کشور شده‌اند. یکی از اولین مواردی که باید پس از نصب مودم‌های بی سیم به آنها توجه کرد، رمزگذاری روی آنها به منظور جلوگیری از سوء استفاده از سرویس اینترنت توسط کاربران ناخواسته است؛ اما حتی اگر شما به اهمیت استفاده از رمز روی مودم هم واقف باشید باز هم ممکن است بررسی تفاوت بین روش‌های مختلف رمزنگاری برایتان پیچیده بوده و خارج از حوصله شما باشد. در هر صورت به احتمال بسیار زیاد حتی اگر این تفاوت‌ها را هم ندانید با اسامی مخفی نظیر WEP، WPA و WPA2 آشنا هستید؛ اما هر کدام از این موارد به چه معنی هستند و کدام یک امنیت بیشتری را برای شبکه شما فراهم می‌کنند؟

تفاوت‌های واقعی یا ظاهری؟

اگر دستگاه مودم را از فروشنده ای با حوصله خریداری کرده باشید یا اینکه در مراحل نصب آن از افراد با تجربه کمک گرفته باشید حتما از آنها شنیده‌اید که اولین کار پس از روشن کردن مودم و در حال راه اندازی آن، در نظر گرفتن یک رمز عبور است. برای دانستن اهمیت رمزگذاری کافی است شرایطی را در نظر بگیرید که شخصی به صورت غیر قانونی به شبکه شما دسترسی پیدا کرده و به وسیله آن، فعالیت مجرمانه ای را انجام می‌دهد. اگر بتوان این جرم را رهگیری کرد، پلیس مستقیما به منزل یا محل کار شما راهنمایی خواهد شد؛ در حالی که روح شما از اتفاقاتی که افتاده بی اطلاع است. فرضا که تصمیم بگیرید روی شبکه رمز هم بگذارید؛ اما واقعا یک اسم مخفف در کنار این رمز عبور چه تفاوتی می‌تواند ایجاد کند؟ باید بدانید روش‌های مختلف رمزنگاری در واقع سطوح و کارکردهای بسیار متفاوتی با یکدیگر دارند. در درجه اول، با گسترش دسترسی افراد مختلف به شبکه اینترنت، استانداردهای قدیمی به تدریج کاربری خود را از دست داده و در معرض خطر بیشتری قرار می‌گیرند. دانستن تفاوت بین پروتکل‌های مختلف و به کار گیری کاربردی‌ترین و پیشرفته‌ترین آنها بدون شک فرآیندی کلیدی در حفظ اطلاعات شخصی و پشتیبانی از شبکه شما به حساب می‌آید. از اواخر دهه ۹۰ میلادی، الگوریتم‌های امنیتی WiFi شاهد پیشرفت‌های چشمگیر و به روز رسانی‌های گسترده ای بوده‌اند که تقریبا تمامی آنها در ارتباط با کنار گذاشتن الگوریتم‌های قدیمی و بازنگری در راهبردهای امنیتی برای دسترسی به الگوریتم‌های پیشرفته تر و جدیدتر بوده‌اند. به همین دلیل بهترین راه برای شناخت روش‌های رمزنگاری گوناگون، بررسی تاریخچه آنهاست.

Wired Equivalent Privacy – WEP

WEP یا «امنیت مشابه با شبکه‌های با سیم» پر استفاده ترین الگوریتم امنیتی در جهان به شمار می‌رود. دلیل چنین اتفاقی قابلیت Backward Compatibility (سازگاری با شرایط قدیمی تر) و البته این نکته است که WEP اولین گزینه در فهرست روبه روی کاربران برای برقراری یک رمز است. اولین بار در سپتامبر سال ۱۹۹۹ بود که WEP به عنوان یک استاندارد امنیتی WiFi شناخته شد. اولین نسخه‌های WEP حتی در دهه ۹۰ هم آنقدرها قدرتمند نبودند، زیرا محدودیت‌های ایالات متحده روی صادرات تکنولوژی‌های مختلف رمزنگاری باعث شده بود تولید کنندگان محصولات خود را تنها به رمزگذاری‌های ۶۴ بیتی محدود کنند. پس از کنار گذاشتن این محدودیت‌ها، رمزگذاری به ۱۲۸ بیتی ارتقا پیدا کرد و در حال حاضر هم با وجود معرفی رمزگذاری WEP به صورت ۲۵۶ بیتی، باز هم مدل ۱۲۸ بیتی است که بیشترین استفاده را در بین کاربران دارد. رمزی که در حالت ۶۴ بیتی انتخاب می‌کنید، می‌تواند ۵ کاراکتر ASCII (کد استاندارد آمریکا برای تبادل اطلاعات یا آن طور که در زبان فارسی گفته می‌شود؛ اَسکی) یا ۱۰ کاراکتر هگزادسیمال (hex یا دستگاه اعداد پایه ۱۶) باشد، همچنین رمز ۱۲۸ بیتی نیز ۱۳ کاراکتر ASCII یا ۲۶ کاراکتر هگزادسیمال است. با اینکه WEP یک روش رمزگذاری به حساب می‌آید، اما شکستن آن به اندازه ای راحت است که در واقع یک شبکه با رمز WEP تفاوت خاصی با یک شبکه باز ندارد. باوجود باز نگری در این الگوریتم و معرفی حالت ۲۵۶ بیتی، نقص‌ها و ایرادات متعددی در استاندارد WEP کشف شد و بعد تر نیز با افزایش قدرت محاسباتی رایانه‌ها، عبور کردن از WEP آسان تر از قبل شد. در سال ۲۰۰۵ بود که FBI برای آگاه سازی کاربران از ضعف‌های WEP نمایشی عمومی برگزار کرد که در آن به کمک نرم افزارهای رایگان، تنها در عرض کمتر از یک دقیقه رمزهای WEP شکسته می‌شد. در حال حاضر نیز با وجود بهبودهای صورت گرفته، باز هم WEP به شدت آسیب پذیر بوده و به همین دلیل در سال ۲۰۰۴ این روش بازنشسته اعلام شد.

WiFi Protected Access – WPA

دسترسی حفاظت شده به WiFi یا همان WPA یک سال پیش از بازنشستگی WEP و برای جایگزینی آن ارائه شد. پر کاربردترین ساختار استفاده از WPA را می توان WPA-PSK نامید که توسط آن می توان بین ۸ تا ۶۳ کاراکتر ASCII را به عنوان رمز در نظر گرفت. کلیدهای استفاده شده توسط WPA به صورت ۲۵۶ بیتی بوده که پیشرفت چشمگیری نسبت به

حالت‌های ۶۴ و ۱۲۸ بیتی WEP به حساب می‌آیند. برخی از مهم‌ترین تغییرات صورت گرفته توسط WPA عبارتند از بررسی یکپارچگی پیام برای مشخص کردن اینکه آیا مهاجمی توانسته بسته‌های اطلاعاتی رد و بدل شده بین access point و client را تصاحب کند یا خیر و پروتکل یکپارچگی کلیدهای موقت (TKIP). البته بعدتر TKIP با استاندارد رمزنگاری پیشرفته یا AES جایگزین شد. با وجود اینکه WPA برای راحت کردن خیال کاربران و خلاص شدن از WEP طراحی شده بود، اما به دلیل اینکه به وسیله به‌روزرسانی‌های firmware روی دستگاه‌های دارای WEP ارائه می‌شد، باید عناصر مشخصی از آن را تغییر می‌داد که همین موارد در نهایت باعث آسیب پذیری آن می‌شدند. پس از مدتی WPA هم به سرنوشت WEP دچار شد و نمایشی عمومی برای اثبات آسیب پذیری آن اجرا شد.

WiFi Protected Access II – WPA2

در سال ۲۰۰۶ بود که WPA با WPA2 جایگزین شد. یکی از بزرگ ترین تغییرات صورت گرفته در این جایگزینی، استفاده اجباری از الگوریتم‌های AES و همچنین معرفی CCMP (حالت ضد رمز به همراه پروتکل کد اعتبارسنجی پیام تغییر بلوک) به عنوان جایگزینی برای TKIP بود. در حال حاضر استفاده از WPA2 برای کاربران خانگی تقریبا بدون نقطه ضعف بزرگ بوده و عمده نگرانی‌های پیرامون آن به امنیت بخش‌های تجاری مربوط می‌شود. متاسفانه بزرگ ترین نگرانی‌های موجود در WPA همچنان در WPA2 هم حاضرند و با وجود اینکه شکستن دیوار ایجاد شده توسط WPA2 به زمانی بین ۲ تا ۱۲ ساعت کار مداوم در یک رایانه حرفه ای نیاز دارد، اما باز هم ضرورت بازنگری و برطرف کردن حفره‌های امنیتی در آن احساس می‌شود.

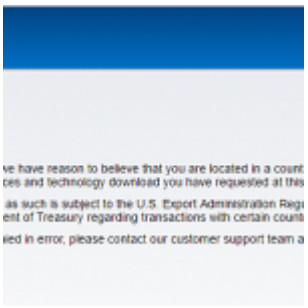
کدام را انتخاب کنیم؟

حالا که با اسامی مختلف این روش‌های رمزگذاری آشنا شدیم باید به این پرسش پاسخ دهیم که در یک شبکه خانگی باید از کدام یک از آنها استفاده کرد؟ اگر بخواهیم خیلی ساده به این سوال پاسخ دهیم، می توان روش‌های رمزگذاری را بر حسب میزان نفوذناپذیری آنها به این صورت در نظر گرفت: قوی‌ترین و امن‌ترین حالت در شبکه‌های خانگی توسط WPA2+AES حاصل خواهد شد. پس از آن به ترتیب می توان WPA+AES، سپس WPA+TKIP/AES، بعد از آن WPA+TKIP، پس از آن WEP و در نهایت شبکه باز و بدون رمزگذاری را نام برد. البته برای استفاده از این

روش‌ها باید یک نکته را در نظر داشت و آن، پشتیبانی تجهیزات شبکه شما از روش‌های مختلف رمزگذاری است. برای مثال اگر از یک مودم قدیمی استفاده می‌کنید ممکن است شرایط به کار گرفتن روش‌های WPA یا WPA2 در آن موجود نباشد و به همین دلیل مجبور شوید از تنظیمات نا امن WEP استفاده کنید. به همین دلیل اگر از این نوع مودم‌ها استفاده می‌کنید حتما به‌روزرسانی‌های امنیتی آن را در وب سایت تولید کننده دنبال کنید و همچنین پیش از خرید یک مودم جدید مطمئن شوید دستگاهی که انتخاب می‌کنید قابلیت به کار گیری روش‌های رمزگذاری جدید را دارد.

منبع:سخت افزار مگ

کمپانی اینتل اجازه استفاده از وب سایت رسمی خود را از ایرانیان گرفت!



همانطور که می دانید،وب سایت های برخی از کمپانی های تولید کننده سخت افزار در ایالات متحده،برای ایران غیر قابل دسترس است.کاربران نیز در این سالها مجبور به استفاده از سامانه هایی بودند که در راستای تغییر IP،آنها را قادر به گذر از این محدودیت می کرد.اما به تازگی اتفاقی بسیار عجیب و غیر منتظره روی داده است که متاسفانه موجب ناراحتی کاربران ایرانی و صد البته،ما شده است.

در حالی که برای سرچ مشخصات فنی یک پردازنده جدید مشغول بودم،متوجه عدم ارتباط با صفحه شده و متوجه شدم که وب سایت رسمی اینتل به نشانی www.intel.com به طور کامل برای کاربران ایرانی

مسدود گشته است!

در ابتدا اینگونه تصور می رفت که این اقدام موقتی بوده و حتی می تواند یک اشتباه باشد.اما متاسفانه کمی بعد،پیام "اینتل" بر روی صفحه اصلی وب سایت منتشر شد که خبر از عدم اجازه به منظور دسترسی IP های ایرانی را اعلام می کرد.پس از باز کردن صفحه اصلی این وب سایت،یک متن کوتاه با شروع واژه We're sorry! مشاهده می گردد.

درخواست شما رد شده است،زیرا ما بر این باور هستیم که شما در کشوری زندگی می کنید که محدودیت های صادراتی ایالات متحده برای آن اجرا شده است.ما از شما معذرت خواهی می کنیم،چرا که هم اینک قادر به ارائه درخواست شما به منظور دستیابی به بخش های نرم افزار،خدمات،دانلودها و تکنولوژی نیستیم.کمپانی اینتل،یک شرکت واقع در آمریکا بوده و تابع قوانین مدیریت صادرات است؛همچنین از قوانین اعلام شده توسط سازمان خزانه داری به منظور تجارت با برخی از کشورها،پیروی می کند.

لازم به ذکر است که کمپانی هایی مانند اینتل و انویدیا که دسترسی وب سایت های رسمی خود را برای کاربران ایرانی مسدود می کنند،علی رغم میل باطنی و اهداف کمپانی،تحت شرایط و قوانین سازمان خزانه داری ایالات متحده دست به این کار می زنند.در نهایت اینتل در پایان این توضیح کوتاه،یادآور شده است که در صورت داشتن اعتراض می توان از آدرس software.intel.com/contact به منظور ارائه شکایت استفاده کرد.شما عزیزان نیز می توانید در مکاتبه خود و در چند خط کوتاه،اعتراض خود به این اقدام خزانه داری ایالات متحده را متذکر شوید.شاید حداقل بهتر از سکوت کامل باشد!

منبع : سخت افزار مگ