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 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.

از ترفند عجیب ویندوز ۱۰ جا نمانید + آموزش

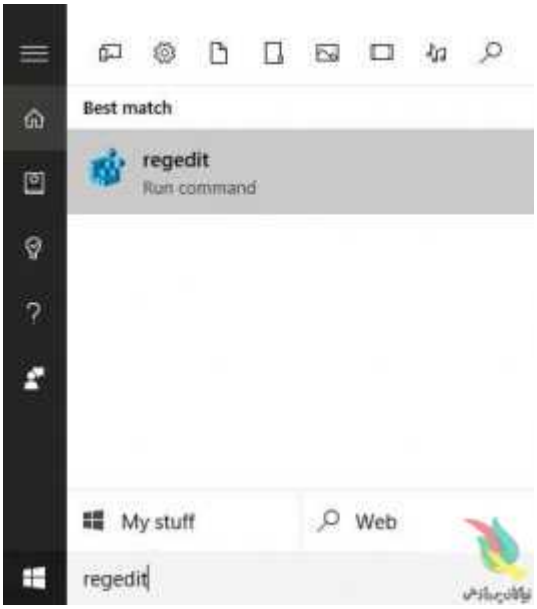
یکی از قابلیت‌های ویندوز ۱۰ امکان تغییر رنگ محیط ویندوز به رنگ‌های دلخواه کاربر است، اما اگر دوست داشته باشید رنگ Start Menu بدون توجه به رنگ بخش‌های دیگر همواره تیره باشد، می توانید با راه‌حلی که برای شما داریم این کار را انجام دهید.

مایکروسافت نام تم‌های رنگی ویندوز را Accent گذاشته است تا رنگ قسمت‌های مختلف به انتخاب کاربر تغییر کند، اما اگر نخواهید این رنگ‌ها را در نوار وظیفه و استارت منو ببینید چه راهی وجود دارد؟ متاسفانه در این صورت نمی‌توانید از هیچ رنگی استفاده کنید ، اما نگران نباشید زیرا با کمی دستکاری در رجیستری ویندوز ۱۰ می‌توانید از تم رنگی به همراه استارت منو تیره بهره ببرید.

برای بهره بردن از چنین روشی، مراحل زیر را به ترتیب انجام دهید:
۱. بخش Settings را باز کنید و سپس وارد قسمت Personalization شوید. در پایین‌ترین قسمت از تب Colors، گزینه «Automatically pick an accent color from my background» را در حالت Off قرار

دهید.

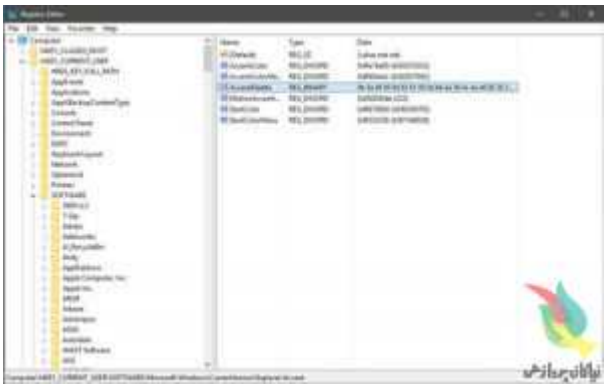
۲. با تایپ «regedit» در نوار جستجو/کورتانا، رجیستری ویندوز را اجرا کنید.



۳. پس از باز شدن رجیستری به مسیر

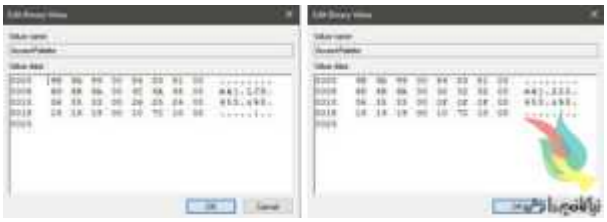
HKEY_CURRENT_USER>SOFTWARE>Microsoft>Windows>
CurrentVersion>Explorer>Accent

بروید.



۴. از بخش سمت راست، کلید «AccentPalette» را انتخاب کنید و سپس با استفاده از مسیر File>Export از کلید مربوط به پلت رنگ بک‌آپ بگیرید.

۵. حالا تنظیمات کلید «AccentPalette» را باز کنید و مقدار داخل ستون‌های ۵، ۶ و ۷ از سطر دوم را به ۳۲ و مقدار داخل ستون‌های مشابه از سطر سوم را به ۰F تغییر دهید.



۶. حالا روی گزینه OK کلیک کنید، سپس کامپیوتر خود را ریست کنید. پس از ریست نوارهای عنوان رنگی و سایر بخش‌ها مانند استارت منو، نوار وظیفه و action center تیره خواهند شد.

پس از انجام مراحل بالا، در صورتی که از نتیجه راضی نبودید با قرار دادن گزینه مرحله شماره ۱ را در حالت On قرار دهید.

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

آموزش غیر فعال کردن جلوه های تصویری در ویندوز ۱۰(برای

افزایش سرعت ویندوز)

ویندوز ۱۰ دارای جلوه های انیمیشنی است تا محیط کاربری زیباتری را برای کاربران ایجاد کند. اما این جلوه های گرافیکی و انیمیشنی ها ممکن است باعث ناراحتی بعضی کاربران حرفه ای شود که نیاز به سرعت عملکرد بالا در ویندوز دارند. چون این جلوه های تصویری بخشی از منابع سیستم را اشغال کرده و سرعت سیستم را کاهش میدهند.

در ادامه مطلب روش غیر فعال کردن جلوه های تصویری ویندوز ۱۰ را آموزش خواهیم داد.

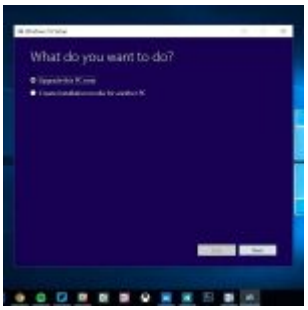
ابتدا Settings ویندوز ۱۰ را از طریق منوی استارت باز کنید.

سپس قسمت Ease of Access را انتخاب کنید.

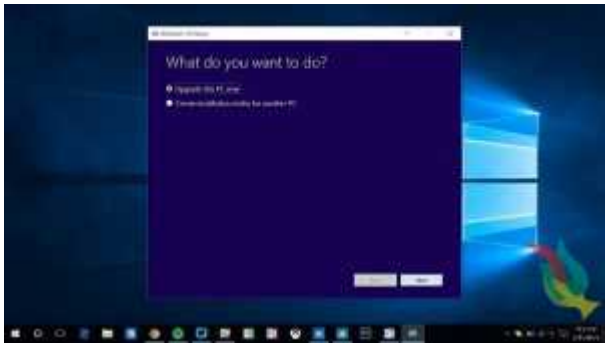
از بخش Other Options اهرم گزینه Play animations in Windows را به سمت چپ هدایت کنید تا وضعیت آن Off شود.

اکنون حالت انیمیشن برای کل ویندوز غیرفعال شده و تمامی پنجره ها و صفحه استارت به صورت ساده و بدون انیمیشن باز خواهد شد.

مایکروسافت نصب ویندوز ۱۰ و حذف نرم افزارهای پیش فرض را آسان می کند



مایکروسافت در حال تست یک ابزار تازه برای نصب آسان تر ویندوز ۱۰ روی رایانه های رومیزی است. در شرایطی که نسخه جدید ویندوز امکان "reset" یک رایانه و بازگرداندن آن به تنظیمات اولیه را در اختیار کاربران قرار می دهد، ابزار جدید می تواند تمام نرم افزارهای اضافه ای که تولیدکننده کامپیوتر روی آن نصب کرده را حذف و یک نسخه تمیز از ویندوز ۱۰ را دوباره نصب نماید.



بیشترین کاربرد ابزار جدید برای رایانه های تازه خریداری شده است که شما می توانید با استفاده از آن از دست تمام نرم افزارهای پیش فرض کارخانه ای خلاص شوید.

این ابزار فعلاً تنها در اختیار کاربران عضو ویندوز اینسایدر قرار دارد، اما گمان می رود که فاصله زیادی تا عرضه عمومی آن نداشته باشیم. به طور قطع کاربران بسیاری از این امکان جدید استقبال می کنند، به خصوص که فاصله چندانی با عرضه آپدیت بزرگ سالیانه

ویندوز ۱۰ در تابستان نداریم.

علاوه بر ابزار مذکور، مایکروسافت در حال ایجاد تغییراتی در ویندوز ۱۰ موبایل است؛ قابلیت Kids Corner به دلیل عدم استقبال کاربران حذف خواهد شد، اما در عوض ویژگی Apps Corner حفظ می گردد تا کاربران همچنان بتوانند پروفایل های محدود شده ای را برای دسترسی از پیش تعیین شده به برخی نرم افزارها ایجاد نمایند. لازم است اضافه نماییم که این شخصی سازی شامل «صفحه استارت» نیز خواهد شد.

منبع:رایان صبا

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

SSD چیست و چگونه کار می‌کند؟ (قسمت اول)

SSDها نوع نسبتا جدید و بسیار سریعی از حافظه هستند که نسبت به هارد دیسک‌ها دارای سرعت و امنیت انتقال داده‌ی بالاتری هستند. اما این حافظه‌ها معایبی از جمله قیمت بالا و کند شدن به مرور زمان دارند. با ما باشید تا با هم به بررسی نحوه‌ی عملکرد این حافظه‌ها بپردازیم.

درایوهای حالت جامد نوعی از حافظه‌ی سریع و قابل‌حمل بوده که در پی تصاحب جایگاه هارد دیسک‌ها هستند. این حافظه‌ها انواع مختلفی دارند که همگی بر پایه سلول فلش ناند هستند. همیشه شاهد بحث و گفتگو بین دوستداران تکنولوژی در مورد مزایا و معایب انواع ساختارهای NAND از جمله NAND مسطح در مقابل NAND عمودی یا MLC یا سلول چند لایه(Multi Level Cell) در مقابل TLC یا سلول سه لایه(Triple Level Cell) بوده‌ایم. برای آشنایی بیشتر با SSDها، چند سوال در مورد حافظه‌های ذخیره سازی می‌پرسیم و سپس به تک تک آنها جواب می‌دهیم. SSDها با حافظه‌های مبتنی بر دیسک چرخان متفاوت هستند. بنابراین پیش از آشنا شدن با SSD ها، لازم است که ابتدا با هارد دیسک‌ها آشنا شویم.

هارد دیسک چیست و چگونه کار می‌کند؟

یک هارد دیسک(Hard Disc Drive)، اطلاعات را بر روی دیسک‌های مغناطیسی چرخان ذخیره می‌کند. این دیسک‌های مغناطیسی را پلاتر (Platter) می‌نامند. در درون هر هارد دیسک یک بازوی فعال‌کننده نیز وجود دارد که سرهای مخصوص خواندن و نوشتن اطلاعات بر روی آن سوار هستند تا به همه‌جای دیسک دسترسی داشته باشند. بازوی مورد نظر، هنگام نیاز به خواندن یا نوشتن اطلاعات، این سرهای مخصوص خواندن و نوشتن را در مکان مناسب بر روی دیسک مغناطیسی قرار می‌دهد تا اطلاعات خوانده یا نوشته شوند.

از آنجا که برای خواندن یا نوشتن اطلاعات یا اجرای یک برنامه‌ی خاص، سرهای درایو باید اطلاعات را از روی دیسک استخراج کرده یا روی آن بنویسند، و از آنجا که این دیسک دائم در حال چرخش است، مدت زمانی طول می‌کشد تا سرها دقیقا بر روی نقطه‌ی مورد نظر قرار گرفته و عملیات استخراج یا نوشتن داده را آغاز کنند. ممکن است که برای استخراج داده، نیاز باشد که اطلاعات از چندین جای مختلف دیسک خوانده شوند. در این صورت دیسک باید چندین بار چرخیده و هربار یکی از نقاط مورد نظر را در مقابل سرهای مخصوص قرار دهد تا اطلاعات خوانده یا نوشته شوند. اگر درایوی در حالت خواب (Sleep) یا حالت انرژی کم (Low Power Mode) باشد، از آغاز به حرکت آن تا رسیدنش به حداکثر سرعت برای انتقال داده، چند ثانیه طول می‌کشد.

از ابتدا معلوم بود که هارد دیسک‌ها توانایی آن را ندارند که با سرعت پردازنده‌ها کار کرده و پا به پای آن‌ها جلو بیایند. تاخیر در هارد دیسک‌ها با میلی ثانیه سنجیده می‌شود؛ در حالی که در پردازنده‌ها، تاخیر در حد چند نانو ثانیه است. بنابراین تاخیر هارد دیسک‌ها چند میلیون برابر پردازنده‌ها است! برای یک هارد معمولی حدود ۱۰ الی ۱۵ میلی ثانیه زمان نیاز است تا اطلاعات را بر روی دیسک یافته و شروع به خواندن آن‌ها کند. با این حال صنعت هارد دیسک تمام تلاش خود را کرده است تا سرعت این محصولات را بالا ببرد. از جمله این تلاش‌ها می‌توان به کاهش اندازه‌ی پلاترها، افزایش سرعت گرداننده‌ی دیسک و استفاده از حافظه‌ی کش(Cache) بر روی دیسک اشاره کرد. با وجود این تلاش‌ها، سریع‌ترین هارد دیسک‌های قابل استفاده برای کاربران عادی در جهان، خانواده‌ی هاردهای VelociRapors شرکت وسترن دیجیتال هستند که دارای سرعت چرخش ۱۰,۰۰۰ دور بر دقیقه هستند. هارد دیسک‌هایی نیز وجود دارند که سرعت چرخش ۱۵,۰۰۰ دور بر دقیقه دارند، اما برای کاربران عادی قابل استفاده نیستند. مشکل هارد دیسک‌ها این است که حتی سریع‌ترین نمونه‌های آنها در جهان نیز سرعتشان در مقایسه با پردازنده‌ها آن قدر کم است که حتی قابل درصد دهی هم نیست!

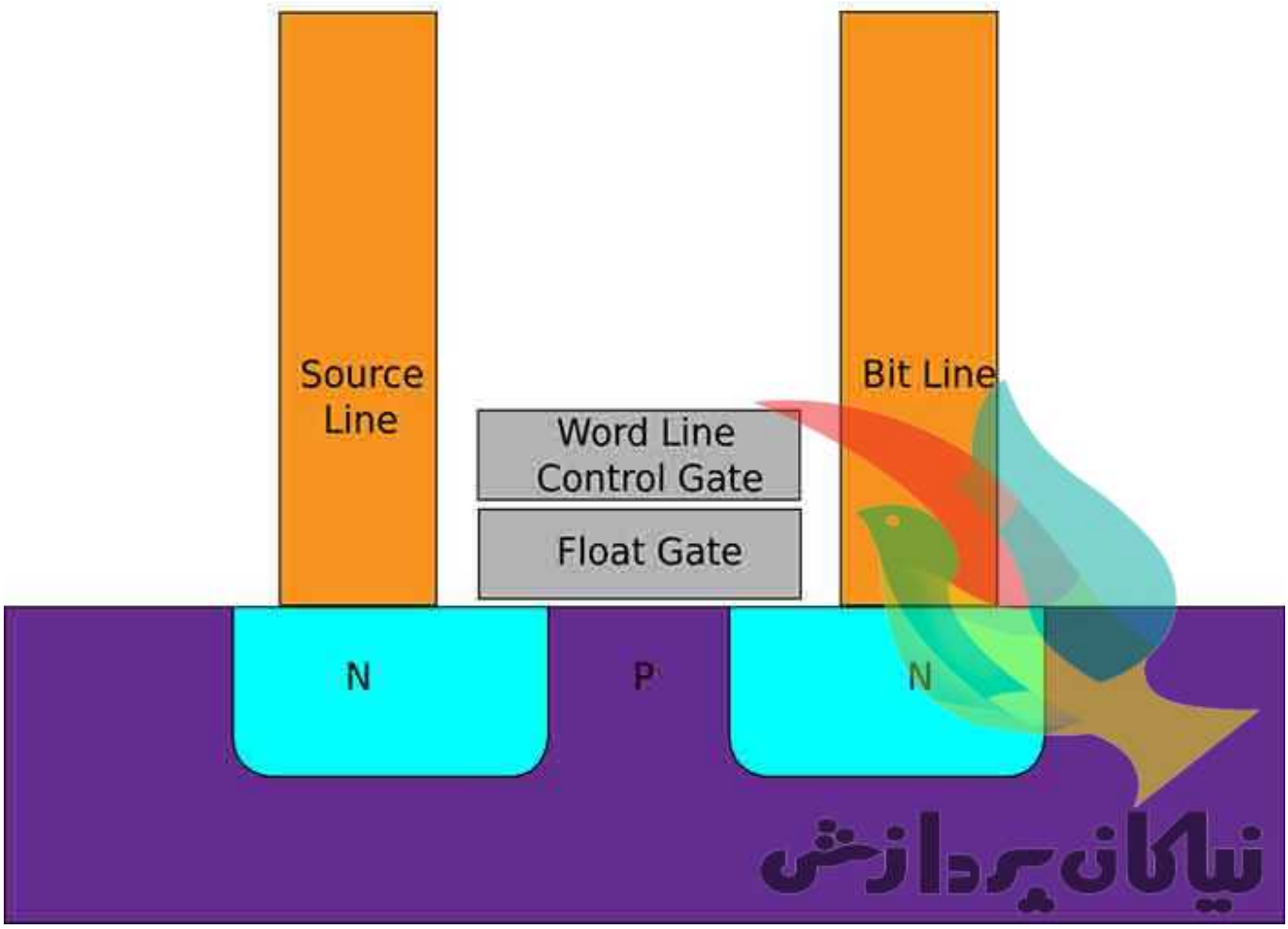
SSD ها چگونه کار می‌کنند؟

هنری فورد، پس از فروختن صدها هزار اتومبیل در آمریکا، در جواب سوال فردی که از او علت وارد شدنش به عرصه‌ی اتومبیل سازی را پرسید گفت: «اگر از مردم می‌پرسیدم که چه چیزی می‌خواهند، آن‌ها جواب می‌دادند: اسب‌های سریع‌تر!»

حال پس از گذشت ۱۰۰ سال انسان‌های امروزی هم به سریع‌ترین منتقل کننده‌ها احتیاج دارند. البته منتقل‌کننده‌ی داده‌ها و اطلاعات، نه افراد!

SSD یا درایو حالت جامد(Solid State Drive) را به این دلیل با این نام می شناسند که بر خلاف هارد دیسک‌ها، ساز و کار آن مبتنی بر چرخش اجسام و حرکت اجرای داخلیش نیست. در SSDها، اطلاعات به جای دیسک چرخان، در دریایی از فلش ناند ذخیره می‌شوند. ناند خود از اجزایی ساخته شده است که ترانزیستورهای گیت شناور نامیده می‌شوند. بر خلاف ترانزیستورهای استفاده شده در ساخت DRAM یا رم پویا (Dynamic Random Access Memory) که باید هر ثانیه چندین بار رفرش

شوند، فلش ناند به گونه‌ای طراحی شده است که حتی اگر منبع انرژی در دسترسش نباشد باز هم بتواند حالت شارژ یا دشارژ خود را حفظ کند. همین امر موجب شده است که ناند را در دسته‌ی حافظه‌های غیر فرار دسته‌بندی کنند.



شکل بالا، طرح ساده‌ای از یک سلول فلش را نشان می‌دهد. الکترون‌ها در گیت شناور ذخیره شده و کنترلر فلش با خواندن مقادیر صفر و یک که به ترتیب به معنی شارژ و دشارژ بودن سلول است وضعیت آن را تعیین می‌کند. صفر و یک اینجا با ذهنیت قبلی ما از این دو عدد متفاوت هستند. در فلش ناند، صفر به معنای آن است که داده در سلول ذخیره شده است و یک بدین معناست که سلول خالی است. فلش ناند در یک شبکه‌ی توری مانند و مشبک به صورت منظم چیده می‌شود. به هرکدام از لایه‌هایی که شبکه را می‌سازند، صفحه (Page) و به کل این شبکه توری مانند، بلوک می‌گویند. اندازه‌های متداول برای صفحات عبارت است از

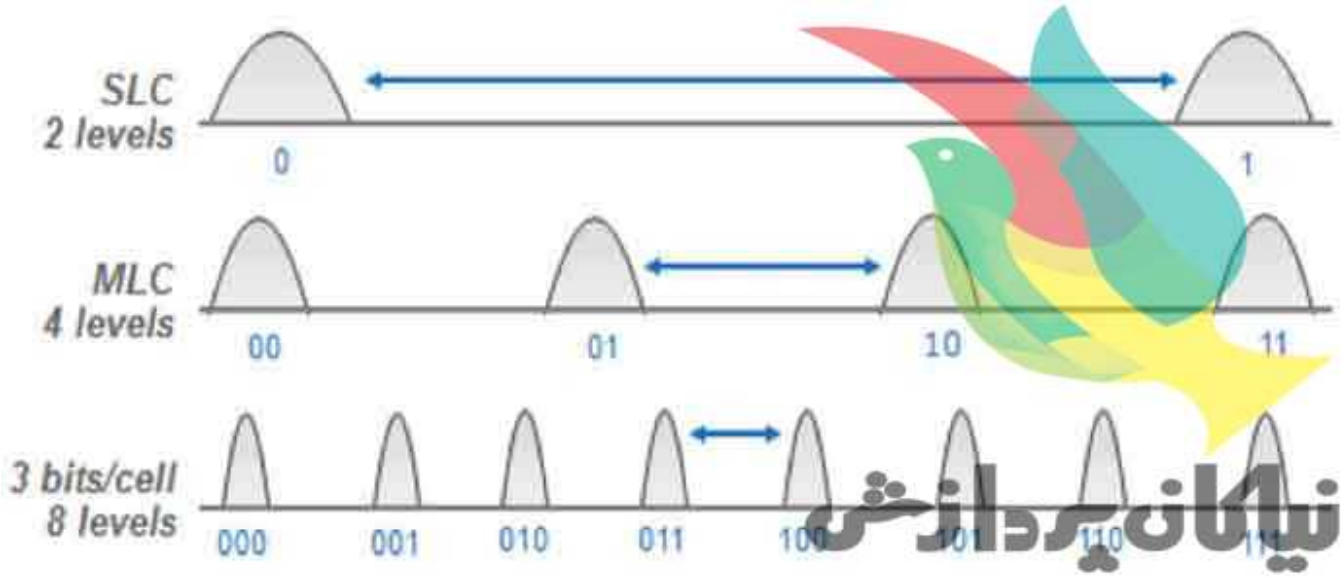
۲۰۰۰، ۴۰۰۰، ۸۰۰۰ و ۱۶۰۰۰ سلول. در هر بلوک نیز ۱۲۸ یا ۲۵۶ صفحه قرار دارد. پس با این حساب، گنجایش هر بلوک حداقل ۲۵۶ کیلوبایت و حداکثر ۴ مگابایت است. یکی از مزایای SSDها، سرعت بسیار بالاتر آن‌ها نسبت به هارد دیسک‌ها است. از آنجا که در درون SSDها هیچ‌گونه قطعه‌ی متحرکی وجود ندارد، تاخیر کمتر بوده و سرعت انتقال داده بالاتر می‌رود. جدول زیر، میزان تاخیر دسترسی را در انواع حافظه‌های معمول بر حسب میکروثانیه نشان می‌دهد.

	SLC	MLC	TLC	HDD	RAM
P/E cycles	100k	10k	5k	*	*
Bits per cell	1	2	3	*	*
Seek latency (µs)	*	*	*	9000	*
Read latency (µs)	25	50	100	2000-7000	0.04-0.1
Write latency (µs)	250	900	1500	2000-7000	0.04-0.1
Erase latency (µs)	1500	3000	5000	*	*
Notes	* metric is not applicable for that type of memory				
Sources	P/E cycles [20] SLC/MLC latencies [1] TLC latencies [23] Hard disk drive latencies [18, 19, 25] RAM latencies [30, 52] L1 and L2 cache latencies [52]				

نیکان پردازش

NAND از نظر سرعت اصلا قابل مقایسه با حافظه‌های رم نیست؛ اما در مقایسه با هارد دیسک‌ها بسیار سریع‌تر است. حتی با وجود آن که سرعت نوشتن حافظه‌های NAND در مقایسه با سرعت خواندنشان کمتر است، باز هم در این زمینه بسیار سریع‌تر از هارد دیسک‌ها هستند. دو نکته در

مورد شکل بالا وجود دارد. اول اینکه با کمی دقت می‌توان فهمید که هرچه تعداد بیت‌ها در سلول فلش بالاتر می رود، تاخیر در آن به طور قابل ملاحظه‌ای افزایش می یابد. تاثیر این کند شدن بر روی نوشتن، بیشتر از خواندن است. مثلا تاخیر خواندن در سلول سه لایه (TLC) نسبت به سلول تک لایه (SLC) حدودا ۴ برابر است؛ اما تاخیر نوشتن در سلول سه لایه، ۶ برابر تاخیر نوشتن در سلول تک لایه است. با افزایش تعداد بیت‌ها در هر سلول فلش، تاخیر در پاک کردن داده‌ها هم همانند نوشتن و خواندن بسیار بیشتر می‌شود. اگر تعداد بیت‌ها n برابر شود، لزوما تاخیر هم n برابر نمی‌شود؛ بلکه بیشتر از n برابر می‌شود. مثلا اگر به سلول سه لایه نگاه کنیم می‌بینیم که دو برابر سلول دولایه تاخیر دارد؛ در حالی که تعداد بیت‌های آن تنها ۵۰ درصد بیشتر از تعداد بیت‌های سلول دولایه است.



دلیل کندتر بودن سلول سه لایه نسبت به سلول‌های دو لایه و تک لایه، نحوه‌ی حرکت اطلاعات در بیرون و داخل سلول است. در سلول تک لایه، تنها اطلاعاتی که کنترلر نیاز دارد این است که بداند بیت متناظر با وضعیت سلول، صفر است یا یک. در سلول دو لایه، به دلیل وجود دو بیت، چهار حالت مختلف ارزش را داریم: ۰۰، ۰۱، ۱۰ و ۱۱. سلول سه لایه نیز می‌تواند هشت ارزش مختلف داشته باشد. برای خواندن ارزش سلول از بیرون، کنترلر حافظه باید ولتاژ بسیار دقیق و حساب شده‌ای را به درون سلول یک لایه یا گروه دو یا سه‌تایی سلول‌ها بفرستد تا با گرفتن فیدبک بتواند تعیین کند که کدام سلول شارژ شده و کدام یک شارژ نشده است.

خواندن، نوشتن و پاکسازی داده در SSDها چگونه انجام می‌شود؟

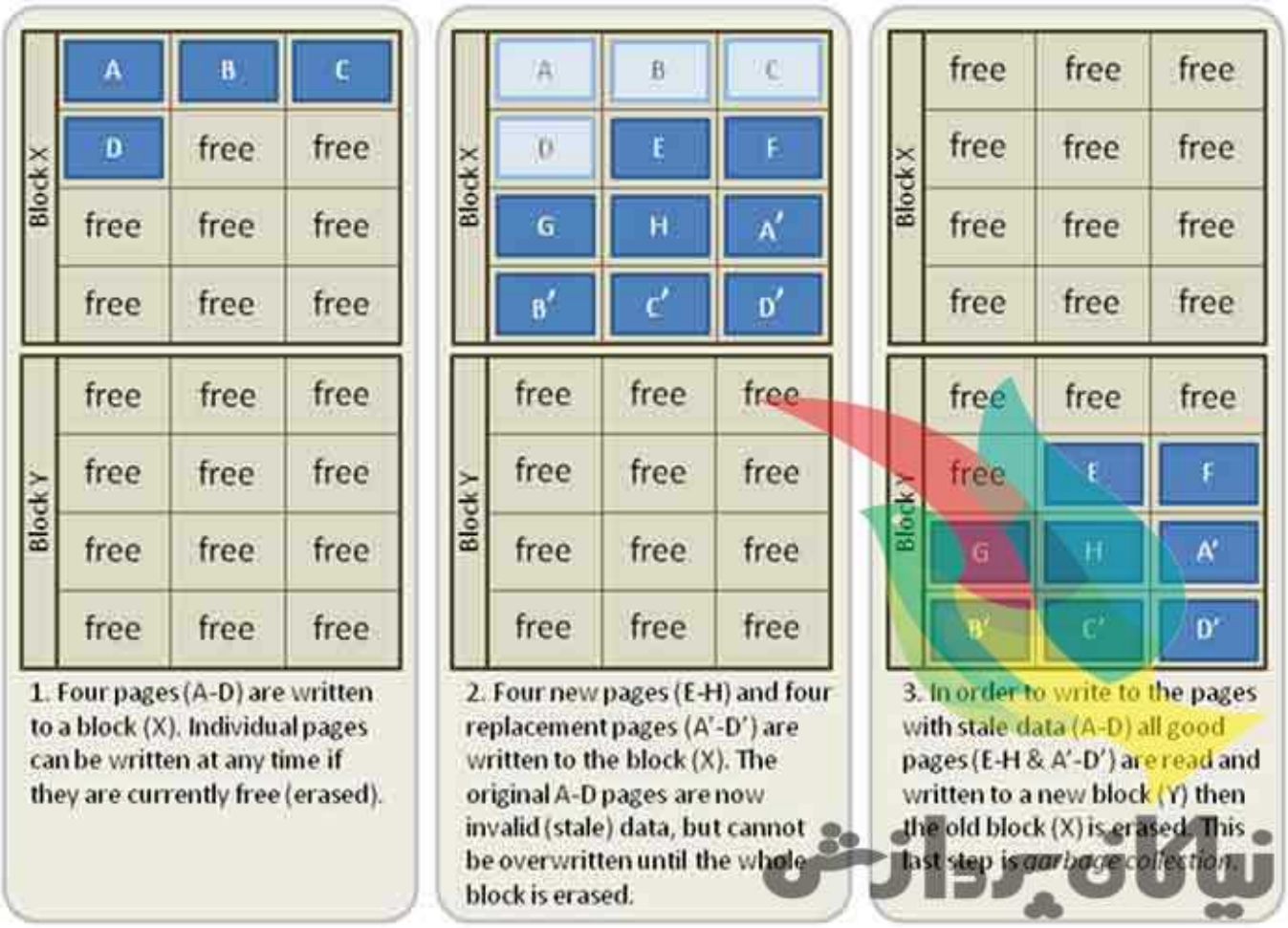
یکی از مشکلات SSDها این است که اگرچه می‌توانند اطلاعات را با سرعتی بسیار بالا در درایوهای خالی بنویسند، اما در صورت نوشتن مقادیر زیادی از اطلاعات، به مرور زمان دچار کندی می‌شوند. دلیل این کندی به یکی از ویژگی‌های منحصر به فرد SSDها بر می گردد. SSDها می‌توانند داده را از یک صفحه بخوانند یا در یک صفحه بنویسند. اما اگر نیاز به پاک کردن اطلاعات یک سلول باشد، نمی‌توانند تنها اطلاعات آن سلول یا حتی آن صفحه را پاک کنند؛ بلکه تمام اطلاعات موجود در آن بلوک را حذف می‌کنند. زیرا فرض را بر خالی بودن صفحات مجاور می‌گذارند. دلیل این انتخاب این است که برای پاک کردن اطلاعات از روی صفحات فلش ناند، ولتاژ زیادی لازم است و اگر به صورت نظری بتوان اطلاعات یک صفحه را پاک کرد، ولتاژ بالای اعمال شده در آن، صفحات مجاور را نیز تحت‌تاثیر قرار داده و اطلاعات ذخیره شده در آنها بر اثر این ولتاژ بالا دستکاری و غیر قابل استفاده می‌شوند. بنابراین بهترین راه این است که داده‌ها را به صورت بلوکی حذف کنیم تا این مشکل برطرف شود. اما SSDها برای بازنویسی اطلاعات در یک صفحه چگونه عمل می‌کنند؟ SSDها این کار را در سه مرحله انجام می‌دهند:

- مرحله‌ی اول، کپی کردن تمام اطلاعات بلوکی است که صفحه‌ی مورد نظر ما در آن واقع شده است
- مرحله‌ی دوم، پاک کردن تمام اطلاعات داخل بلوک است
- مرحله‌ی سوم هم «نوشتن اطلاعات کپی شده + اطلاعات مورد نظر ما» در بلوک و صفحه‌ی مورد نظر است.

بدین ترتیب بدون کوچکترین تغییری در دیگر اطلاعات بلوک، توانسته‌ایم اطلاعات یک صفحه را به روز کنیم. اگر درایو پر باشد و هیچ صفحه‌ی خالی در دسترس نباشد، SSD باید ابتدا به دنبال بلوک‌هایی بگردد که قبلا آنها را به عنوان بلوک حذف شده علامت‌گذاری کرده، اما اطلاعات داخلشان را حذف نکرده است. پس از یافتن این بلوک‌ها، آن‌ها را پاک کرده و سپس اطلاعات را در صفحه مورد نظر که حالا خالی است بنویسد. دلیل کند شدن SSDها پس از گذشت زمان نیز همین است. یک درایو SSD تقریبا خالی، دارای بلوک‌های خالی بسیار زیادی است که می‌تواند اطلاعات را در آنها بنویسد. به همین دلیل سرعت خیلی زیادی دارد. اما یک SSD تقریبا پر، به احتمال بسیار

زیاد باید برای نوشتن اطلاعات، چندین بار چرخه‌ی نوشتن و پاک‌کردن (program/erase cycle) بالا را طی کند و به همین دلیل سرعتش پایین می‌آید. استفاده از آخرین مگابایت‌های باقی‌مانده‌ی یک SSD واقعا آزار دهنده است.

اگر تاکنون از SSD استفاده کرده‌اید، به احتمال زیاد عبارت جمع‌آوری زباله(Garbage Collection) را هم شنیده‌اید. جمع آوری زباله، یک پردازش در پس‌زمینه است که با انجام یک سری پردازش‌های خاص در پس زمینه، به درایو مورد نظر اجازه می‌دهد که از کاهش بیش از حد سرعت در اثر اجرای مداوم چرخه‌ی نوشتن و پاکسازی جلوگیری کند. تصویر زیر به درک بهتر این عملکرد کمک می‌کند.

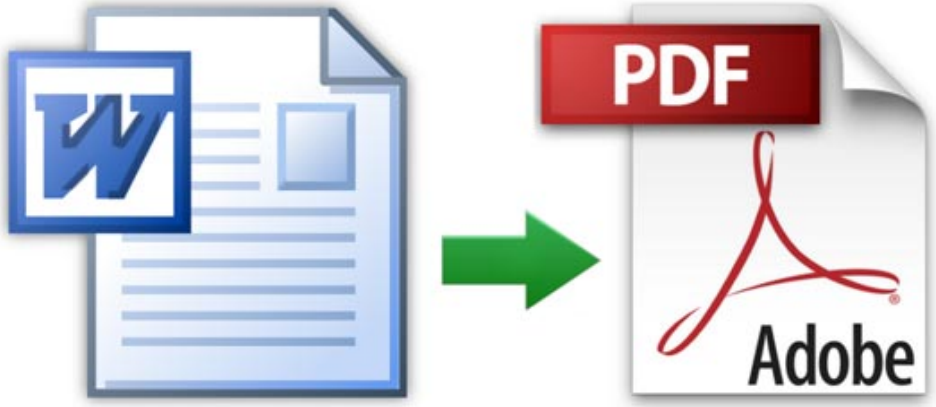


در مورد عکس بالا این نکته را هم مد نظر داشته باشید که این درایو، از این واقعیت بهره گرفته است که با نوشتن ارزش جدید برای چهار بلوک ‘A، ’B، ’C، و ‘D می‌تواند با سرعت بسیار بالایی اقدام به نوشتن اطلاعات در صفحات خالی کند. این درایو همچنین دو بلوک جدید با نام‌های E و H را نیز نوشته است. بلوک‌های A، B، C و D بلوک‌های کهنه محسوب می‌شوند. یعنی اطلاعات موجود در آنها به عنوان

اطلاعات تاریخ مصرف گذشته علامت‌گذاری شده‌اند. هنگامی که درایو مشغول خواندن یا نوشتن اطلاعات نبوده و در حال استراحت باشد، به طور اتوماتیک اطلاعات موجود در صفحات تازه را به یک بلوک جدید منتقل کرده و بلوک یا بلوک‌های قدیمی را پاک می‌کند تا فضای خالی برای اطلاعات جدید آینده ایجاد شود. این بدان معنا است که دفعه‌ی بعدی که SSD نیاز به نوشتن اطلاعات پیدا کند، می‌تواند به جای اجرای چندین باره چرخه‌ی نوشتن و پاکسازی، اطلاعات را مستقیما در بلوک ایکس که اکنون خالی شده است بنویسد.

منبع:زومیت

چگونه فایل‌های Word را به صورت PDF ذخیره کنیم؟!



با آموزش دیگری از مجموعه آموزش های استوار آی تی در خدمت شما هستیم. هرگاه بخواهیم فایلی را ذخیره کنیم که بعدا بتوانیم به راحتی آن را مشاهده کرده و یا اینکه در اینترنت به اشتراک بگذاریم، فایل‌های PDF، مناسب‌ترین گزینه برای ما هستند. این پسوند، به کاربران اجازه می‌دهد تا اسناد خود را بدون دست‌خوردگی و قالبی دل خواه ذخیره کنند و به سایر کاربران نیز امکان می‌دهد تا این فایل را به راحتی در هر سیستمی اجرا کرده و مشاهده نمایند. به همین دلیل، ذخیره نسخه‌های نهایی فایل‌های ورد شما به صورت PDF می‌تواند یکی از بهترین ایده‌های موجود باشد.

در اینجا، نشان می‌دهیم که چه گونه می‌توان در نرم‌افزار Word ورژن‌های ۲۰۱۰ و ۲۰۱۳، اسناد را به صورت PDF ذخیره کرد.

ذخیره فایل Word با پسوند PDF در نرم‌افزار Word2010

۱- مطلب و یا سند خود را تهیه کنید.

۲- بر روی گزینه File کلیک کرده و سپس گزینه Save As را انتخاب کنید.

۳- نامی برای فایل خود انتخاب نمایید. دقت کنید نامی که انتخاب می‌کنید آسان و قابل فهم باشد، انتخاب نامی با استفاده از اعداد و یا حروف نامشخص، شانس شما را برای باز کردن این فایل در آینده کم می‌کند یا حتی ممکن است، هنگام ارسال آن از طریق ایمیل شما را به زحمت بیندازد.

۴- گزینه Save as a Type را انتخاب کرده و سپس گزینه PDF را انتخاب نمایید.

۵- همچنین از گزینه Standard می‌توانید برای پرینت و یا نشر در اینترنت و یا از گزینه Minimum فقط جهت نشر در اینترنت استفاده کنید.

۶- بر روی گزینه Save کلیک کنید.

ذخیره فایل Word به صورت PDF در نرم‌افزار Word 2013

۱- مطلب و یا سندی که بخواهید در آینده از آن پرینت بگیرید، تهیه کنید.

۲- گزینه File و سپس Export را انتخاب کنید.

۳- از منوی بازشده، گزینه Create PDF/XPS را برگزینید.

۴- گزینه Publish را انتخاب کنید.

نرم افزار ورد، یک فایل PDF را از فایل اصلی شما ایجاد کرده و به طور پیش‌فرض با همان اسم قبلی، در فولدر فعلی ذخیره می‌کند.

مواردی که به در هنگام ایجاد فایل PDF باید به خاطر بسپارید:

۱- عدم قابلیت ویرایش فایل

فایل ایجادشده، قابلیت ویرایش و ادیت مجدد را نخواهد داشت. آن هم به این دلیل که فایل ایجادشده، در واقع نوعی طرح و عکس از فایل اصلی شماست. پس معمولا زمانی فایل PDF را ذخیره کنید که ویرایش نسخه نهایی آن به پایان رسیده است. به این ترتیب ویرایش مجدد این فایل بسیار سخت خواهد بود. پس بهتر است، قبل از تبدیل فایل اصلی خود به فرمت PDF، دقیقا آن چیزی را که می‌خواهید ایجاد کرده و تمام ایرادات را بر طرف کنید.

۲- ساده‌ترین راه ویرایش

ساده‌ترین راه ویرایش یک فایل PDF، ویرایش و ادیت فایل اصلی ورد و سپس ذخیره مجدد آن با پسوند PDF است. شما می‌توانید از یک اسم شبیه استفاده کرده و هنگام ذخیره، تنها فایل جدید را با فایل قدیمی جایگزین کنید. اگر فایل قدیمی را در فضای اینترنت آپلود

کردید، می‌توانید به راحتی فایل جدید را با آن جایگزین کنید.

۳- باز کردن فایل PDF و تبدیل آن به فایل Word

برای انجام این کار در مایکروسافت ورد ۲۰۱۳، ابتدا گزینه File و سپس گزینه open را انتخاب نمایید و فایل PDF مورد نظر را باز کنید. در اینجا فایل مورد نظر باید به پسوند ورد تبدیل‌شده و تمامی متون و عکس‌های موجود در فایل به راحتی باز شود. البته احتمال دارد که برخی ویژگی‌های این نوع فرمت غیرفعال باشد که باید برای فعال شدن و درست کار کردن آن، برخی تنظیمات اعمال شود.

۴- اطمینان از فرمت صحیح فایل PDF قبل از ارسال

دقت کنید که تمامی موارد مربوط به قالب‌بندی فایل و یا مشکلات موجود در خصوص فضاهای خالی بین کلمات و… رفع شده باشد. فایل نهایی باید کاملا شبیه فایل اصلی شما باشد.

منبع:http://www.ostovarit.com/single/article/795/چگونه%۲۰فایل‌های%۲۰Word%۲۰را%۲۰به%۲۰صورت%۲۰PDF%۲۰ذخیره%۲۰کنیم؟!