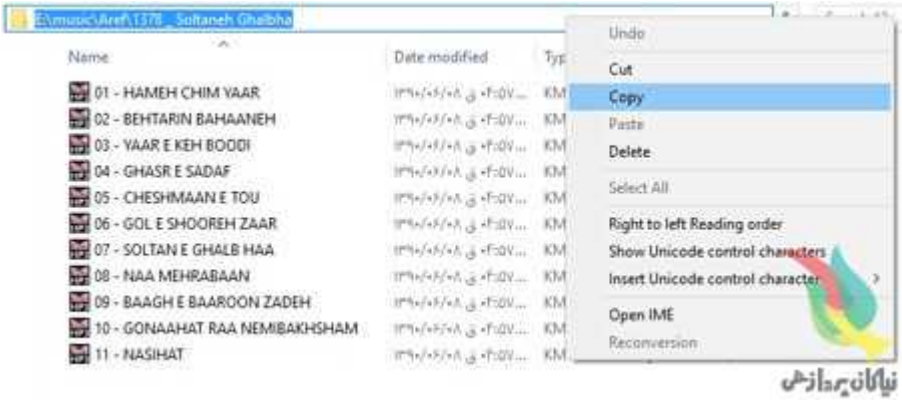
تغییر دسته‌جمعی نام فایل‌ها در محیط ویندوز به کمک اکسل

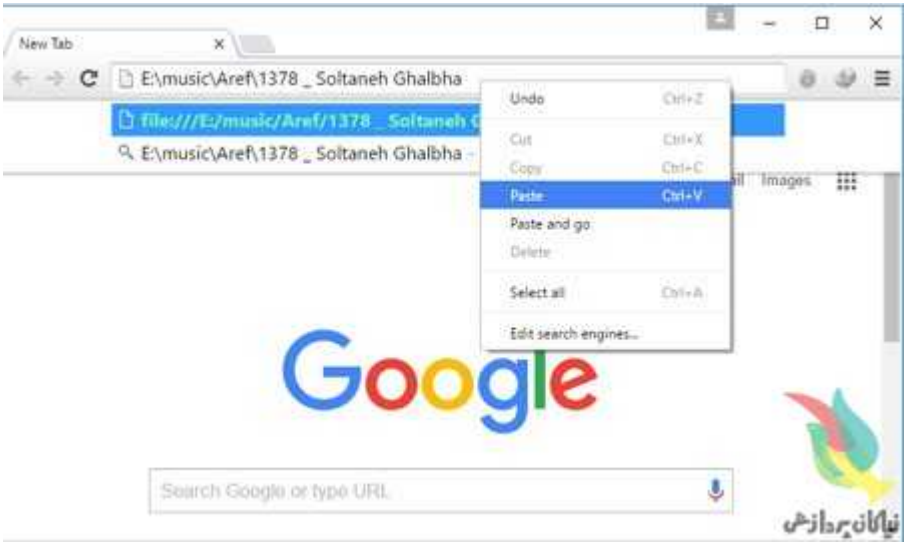


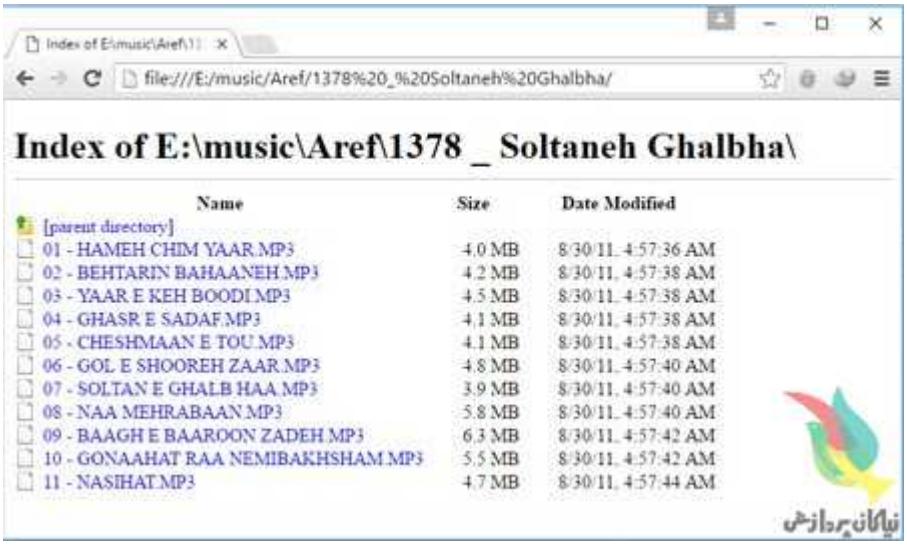
در این ترفند به نحوه‌ی تغییر دسته‌جمعی و یکجای نام فایل‌ها در محیط ویندوز به کمک نرم‌افزار مایکروسافت اکسل و Command Prompt خواهیم پرداخت. این روش از نام‌های فارسی نیز پشتیبانی می‌کند.

ابتدا وارد پوشه‌ای که فایل‌ها در آن قرار دارد شوید. سپس مسیر پوشه را Copy کنید.

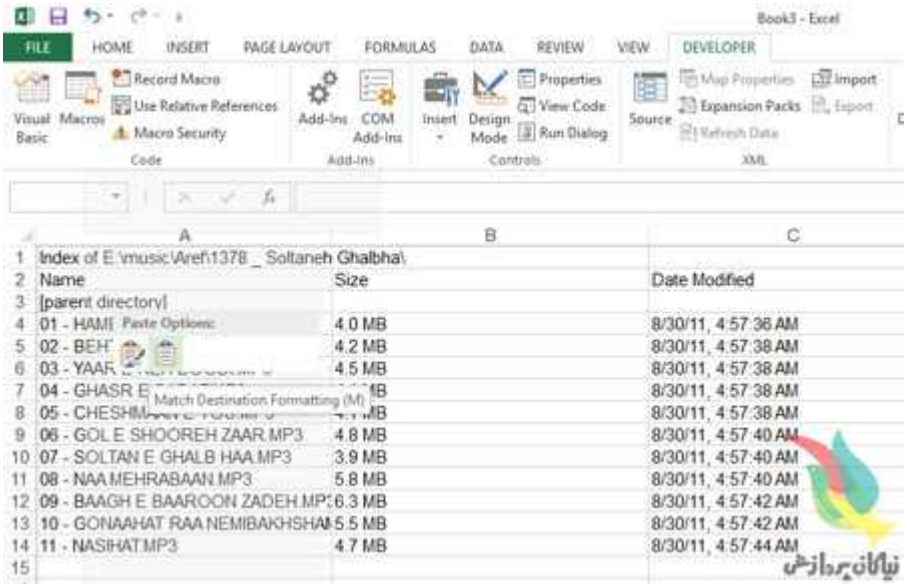


اکنون در مرورگر وب خود، در قسمت نوار آدرس این مسیر را Paste کرده و Enter بزنید.

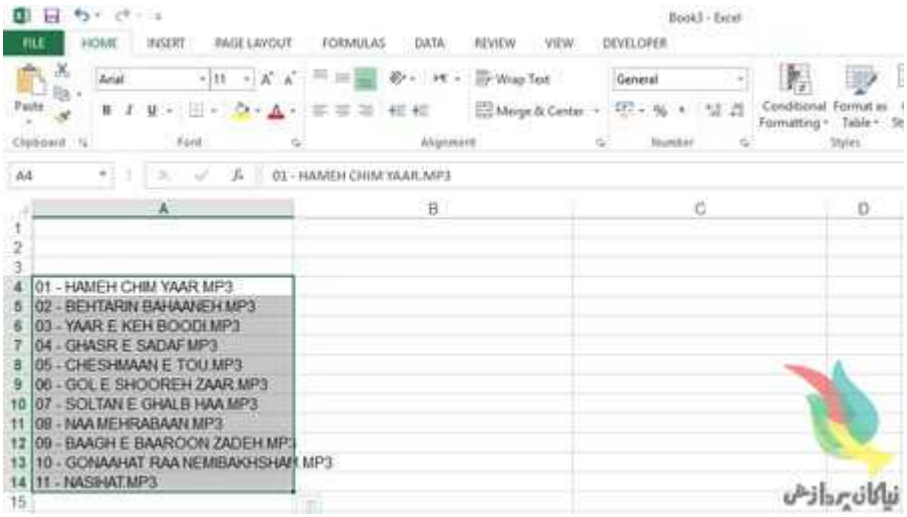




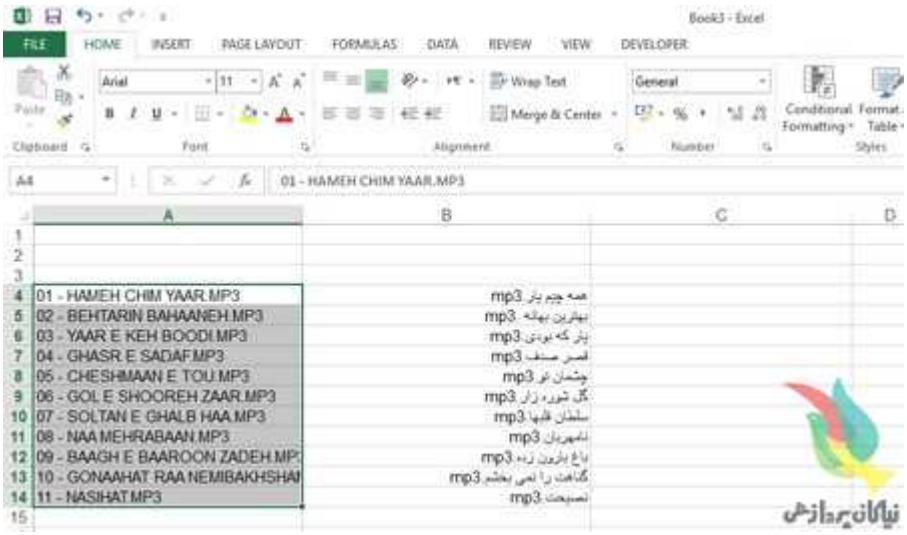
اکنون توسط کلیدهای ترکیبی Ctrl+A کل متون صفحه را انتخاب کرده و آن‌ها را Copy کنید. سپس داخل محیط اکسل در یک صفحه‌ی جدید، این محتوا را Paste نمایید.



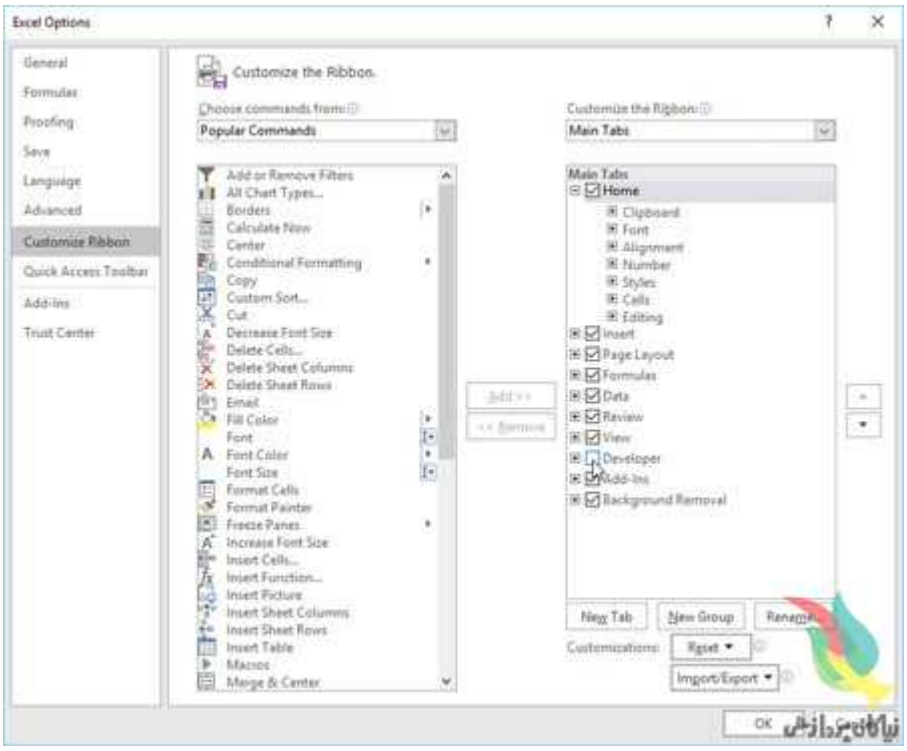
سلول‌های اضافی را پاک نمایید.



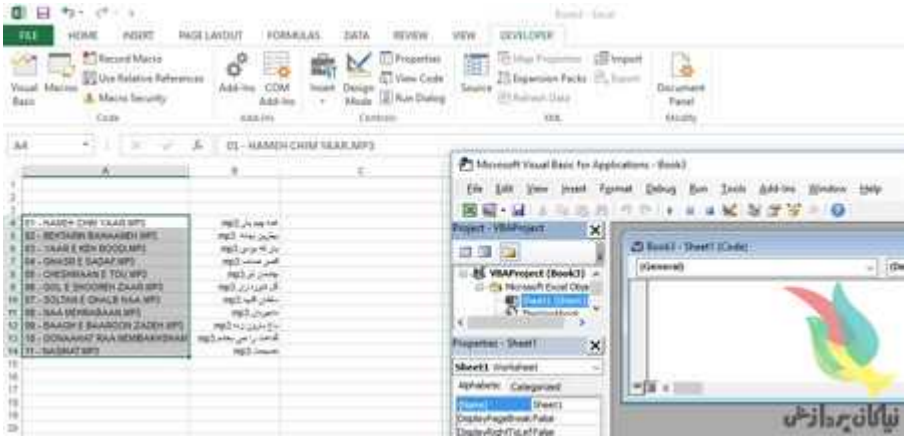
نام جدید با فرمت‌شان را در ستون مقابل بنویسید. سپس ستون نام قدیمی فایل‌ها را انتخاب کنید.



اکنون اگر تب Developer اکسل را تاکنون فعال نکرده‌اید، بر روی File و سپس Options کلیک کنید. سپس در تب Customize Ribbon، گزینه‌ی Developer را فعال کرده و روی OK کلیک کنید.



اکنون در محیط اکسل به تب Developer بروید و Visual Basic را انتخاب کنید (یا کلیدهای Alt+F11 را فشار دهید). سپس روی Sheet1(Sheet1) در سمت چپ دوبارکلیک کنید تا پنجره‌ی سفید رنگ برنامه‌نویسی باز شود.



کد زیر را در کادر سفیدرنگ Paste نمایید:

```
()Sub Macro1

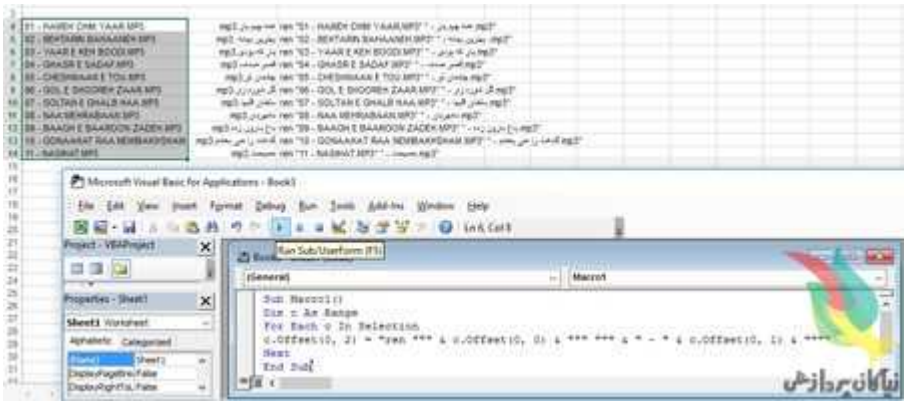
Dim c As Range

For Each c In Selection

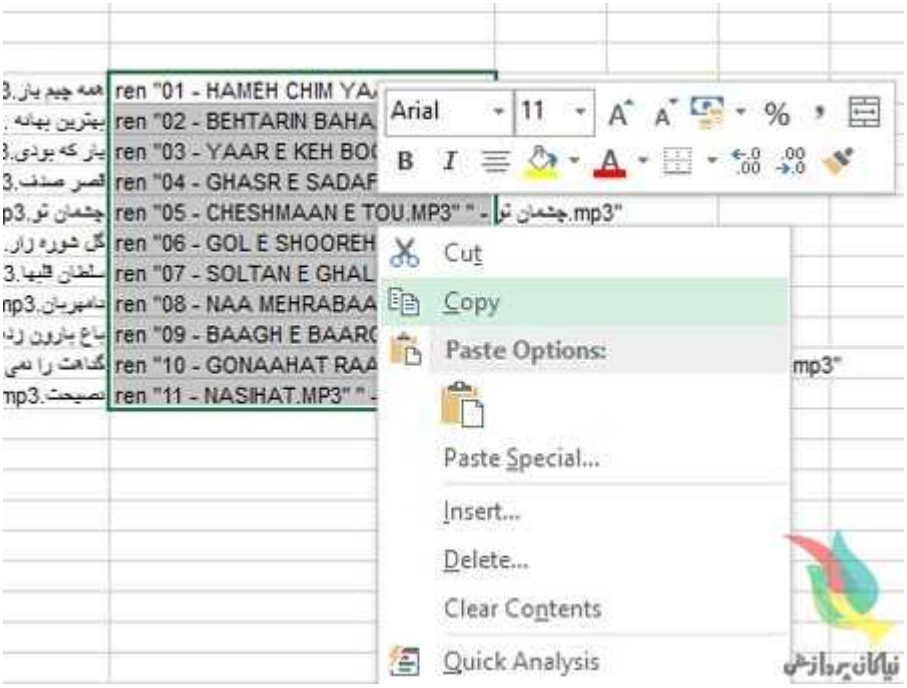
c.Offset(0, 2) = “ren “”” & c.Offset(0, 0) & “”” “”” & ” – ” & “”””” & (c.Offset(0, 1

Next

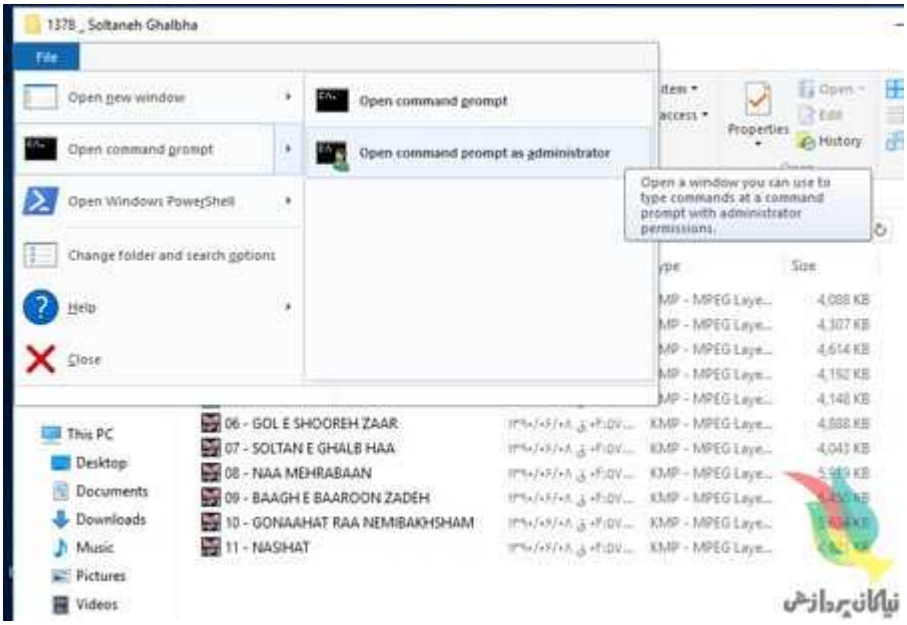
End Sub
```



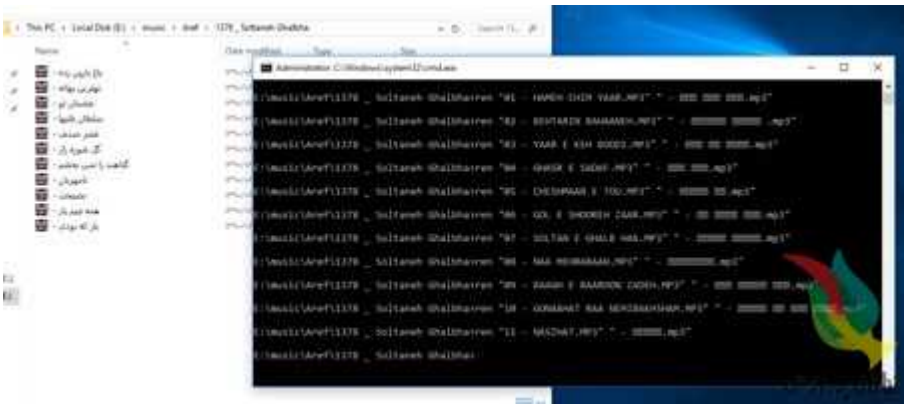
ستون ایجاد شده را Copy نمایید.



به پوشه‌ی مورد نظر بروید و Command Prompt را از منوی File باز کنید.



عملیات Paste را با فشردن کلیدهای Ctrl+V انجام دهید.



تغییر نام فایل‌ها انجام خواهد شد.

منبع: بیتوته

مراقب اطلاعاتتان باشید!



با توجه به حملات سایبری هکرها در چند روز اخیر به سایت های دولتی و شرکت های بزرگ دنیا و حجم خسارات وارد شده به اطلاعات سازمان ها لازم است نکات زیر را رعایت نموده و راهکارهای پیشنهاد شده را با درجه اهمیت بالا انجام دهید:

حملات از نوع باج گیرها می باشند این نرم افزارها بدلیل ماهیت کاری که انجام می دهند از دید آنتی ویروس ها پنهان هستند و اطلاعات اسنادی(Word, Excel, Access, Powerpoint, PDF, E.Mail, SQL, Text) را رمزنگاری می کنند. فایل های رمزنگاری شده صرفا در قبال پرداخت مبالغ زیاد قابل استفاده می باشند و لازم به توضیح است که تاکنون هیچ روشی برای بازگشت و یا بازیابی داده های رمزنگاری شده وجود ندارد.



لازم است نکات پیشگیرانه زیر را مد نظر قرار دهید تا در دام این حملات گیر نیافتید:

۱ – از اطلاعات مهم کاری خود بر روی لوح فشرده CD یا DVD در زمان های متعدد پشتیبان تهیه کنید. توجه داشته باشید که لوح فشرده بعد از عمل رایت(Write) امکان آلوده شدن ندارد.

۲ – تحت هیچ شرایطی ایمیل های مشکوک را باز نکنید. ایمیل های مشکوک عموما با پیشنهادهای مهیجی از قبیل برنده شدن در یک مسابقه یا … می باشد. توجه داشته باشید اینگونه ایمیل ها عموما از آدرس دوستان شما که هک شده اند برای شما ارسال می شود.

۳ – بر روی لینک های خبرهای مهیج مخصوصا در این بازه زمانی که با اخبار انتخابات نیز همراه می شود کلیک نکنید. برای مطالعه اخبار به سایت های معتبر خبرگزاری مراجعه کنید و از باز کردن لینک اخبار یا تصاویر و … در نرم افزارهای شبکه های اجتماعی خودداری کنید.

۴ – به هیچ عنوان از نرم افزارهای شبکه های اجتماعی بر روی سیستم های رایانه ای استفاده کنید. سعی کنید از نسخه های موبایلی آن شبکه ها استفاده کنید.

۵ – آنتی ویروس تان را بروز نگه دارید و از آنتی ویروس های کرک شده استفاده نکنید.

۶ – اگر دستگاه های ذخیره ساز مانند فلش یا هارد اکسترنال به سیستم خود متصل می کنید قبل از بازکردن آن ها را با آنتی ویروس اسکن کنید.

۷ – در صورتی که به باج گیر آلوده شدید(فایل های اسنادی شما به درستی باز نمی شوند و با پیامی مبنی بر رمز شدن اطلاعات مواجه شدید) بلافاصله کابل شبکه را از کامپیوتر خود جدا نمایید.

۸ – تاکید می شود حتما از داده های حساس خود بر روی لوح های CD و یا DVD فایل پشتیبان تهیه نمایید. همچنین می توانید با بهره گیری از نرم افزارهای فشرده سازی چون Winrar فایل های خود را فشرده نموده و ذخیره کنید.

تصویری گویا از علل حملات مهاجمان به گوشی ها





باج افزاری خطرناک با زبان فارسی



تایرنت «TYRANT» باج‌افزار جدیدی است که در روزهای اخیر به‌صورت متمرکز کاربران ایرانی را مورد هدف قرار داده است. این باج‌افزار فارسی براساس یک باج‌افزار متن باز ساخته و توسعه داده شده و اطلاعات کاربران در سیستم‌عامل‌های مایکروسافت ویندوز را برای باج‌خواهی رمزنگاری می‌کند.

سازندگان تایرنت از بستر تلگرام با آدرس @Ttypern و ایمیل ناشناس rastakhiz@protonmail.com برای برقراری ارتباط با قربانی و بررسی پرداخت باج استفاده می‌کنند. این باج‌افزار فایل‌های متنی، تصاویر، ویدیویی و سایر فایل‌های حساس و مهم قربانی با پسوندهای ذکر شده در زیر را رمزنگاری کرده و سپس اقدام به مطالبه ۱۵ دلار باج به شکل ارز الکترونیکی از طریق سرویس Web Money می‌کند و تنها ۲۴ ساعت به قربانی خود مهلت می‌دهد تا مبلغ درخواست شده برای باج را بپردازد. ?



پسوند فایل‌هایی که تایرنت آن‌ها را رمزنگاری می‌کند:

aif, .apk, .arj, .asp, .bat, .bin, .cab, .cda, .cer, .cfg,. .cfm, .cpl, .css, .csv, .cur, .dat, .deb, .dmg, .dmp, .doc, .docx, .drv, .gif, .htm, .html, .icns, .iso, .jar, .jpeg, .jpg, .jsp, .log, .mid, .mp3, .mp4, .mpa, .odp, .ods, .odt, .ogg,.part, .pdf, .php, .pkg, .png, .ppt, .pptx, .psd, .rar, .rpm, .rss, .rtf, .sql, .svg, .tar.gz, .tex, .tif, .tiff, .toast, .txt, .vcd, .wav, .wks, .wma, .wpd, .wpl, .wps, .wsf, ..xlr, .xls, .xlsx, .zip

? مرکز ماهر ایران نیز با انتشار اطلاعیه‌ای در خصوص تایرنت اعلام کرده است که این باج‌افزار از طریق شبکه‌های اجتماعی با فریب دادن کاربران و تشویق آن‌ها به دریافت و اجرای فایل جعلی فیلترشکن سایفون، کاربران ایرانی را مورد هدف قرار داده و در حال انتشار است.

? بررسی‌های اولیه روی تایرنت نشان می‌هد که این باج‌افزار احتمالا نسخه اولیه و آزمایشی از یک حمله بزرگتر است. ضعف در پروسه رمزنگاری فایل‌ها و همچنین وجود برخی خطاها در تغییر تنظیمات ریجستری ویندوز و علاوه بر این، ساختن چندین نسخه آزمایشی مشابه دیگر توسط سازندگان این باج‌افزار، گواه این مساله است. همچنین خوشبختانه درصد قابل توجهی از آنتی‌ویروس‌ها در حال حاضر امکان شناسایی و حذف این باج‌افزار را دارند.

? باید توجه داشت که تایرنت با تکیه بر تکنیک‌های مهندسی اجتماعی قربانی می‌گیرد. استفاده از تکنیک‌هایی فریبنده برای ارائه محتوای آلوده و جعلی که می‌تواند برخی از کاربران را برای دریافت این باج‌افزار و اجرای آن در رایانه‌ها به خطر بیاندازد. برای مثال سازندگان این باج‌افزار پیش‌تر فایل‌هایی آلوده با عناوین فریبنده «khoosoosi shahla-96.EXE» و «pornwatch.EXE» را منتشر کرده‌اند و ماهیت حمله توزیع تایرنت نیز نشان می‌دهد که استفاده از دیگر روش‌های انتشار بدافزار و باج‌افزار، از جمله پیوست ایمیل و از طریق وب‌سایت‌های آلوده نیز امکان‌پذیر است.

حملات اخیر فعلا سیستم های کامپیوتری رو هدف قرار دادن ولی میتونن از طریق دستگاههای دیگه و گوشی های هوشمند و اینترنت و شبکه های مجازی پخش بشن.

این حملات غیرقابل جبران هستند و تمامی اطلاعات مهم سیستم کامپیوتری کد شده و غیرقابل استفاده خواهند شد.

از جمله: عکسها/موزیکها/ویدیوها/فایل های تایپی/نقشه ها/فایل های فشرده شده و هر اونچه که توسط شما یا افراد دیگه ذخیره شده باشه با یه کد مخرب بازنویسی میشن و تا کد بازکننده رو رو بهشون ندین باز نمیشن که این امر هم مسلما در ایران ممکن نبوده و نیست پس:

هر فایلی رو باز نکنین

هر ایمیل ناشناسی رو باز نکنین

به هر چت ناشناسی جواب ندین

عضو هر گروه و کانال ناشناس نشین

هر برنامه کامپیوتری رو از هر کسی قبول نکرده و نصب نکنین.

لطفا به عزیزان تون که در اینترنت گردی تجربه زیادی ندارن اطلاع بدین و بهشون تاکید کنین این حملات شوخی بردار نیستن.

اگر کسی از دوستان یا آشنایان درگیر چنین وضعی شد، حتما و به سرعت سیستم رو خاموش کنه و به هیچ وجه شخصا تلاشی نکنن. حتما سیستم شون رو برسونن به مراکز خدماتی با تجربه که جلوی ضرر بیشتر گرفته بشه و از روشن کردن دوباره سیستم قبل از پاکسازی خودداری کنن.

امیدوارم بتونیم با آگاهی رسانی به موقع از بروز خسارت به خودمون و دوستان مون جلوگیری کنیم.

لطفا آندرویدی ها از CM Security یا Lookout بهره ببرن.

آیفونی ها هم از LookOut یا McAfee یا هر برنامه امنیتی با برند جهانی استفاده کنن.

سیستم های کامپیوتری حتما برنامه امنیتی به روز و معتبر و دارای تاریخ اعتبار داشته باشند.

پیشنهاد من:

Symantec EndPoint Security

Kaspersky

Bitdefender

هست البته نه ویروس یاب اینها بلکه SYSTEM Security یا همون برنامه کامل امنیتی شامل ویروس یاب/ضد هک/ضد اسپم/ضد حملات شبکه ای که معمولا به اسم Total Security یا همون System Security معروف هستند.

از برنامه های دم دستی و تجاری مثل ESET یا Nodو مانند اینها کاری بر نمیاد.

مشکل هنگ کردن ویندوز با تغییر تنظیمات صدا در ویندوز ۱۰





زمانیکه ویندوز هنگ می کند و عملکرد خوبی ندارد بهترین راه نجات استفاده از Task Manager می باشد . پنجره " Task Manager " در ویندوز بهترین دوست کاربر برای رفع مشکلات سیستم عامل می باشد .

این پنجره با ارائه آمار دقیق از عملکرد برنامه و سرویس های در حال اجرا به کاربر کمک می کند فرآیند پردازش را مورد بررسی دقیق قرار بدهد .

در این بخش می توانید مشاهده کنید کدام یک از برنامه ها مقدار مصرف بالای CPU دارد یا به طور مداوم به صورت رندوم توان پردازنده را مورد استفاده قرار میدهد . audiodg.exe یکی از عوامل هنگ کردن سیستم عامل می باشد . Audiodg که اختصار Audio device graph isolation می باشد کار این گزینه تجزیه و تحلیل سخت افزارهای صوتی سیستم عامل می باشد که در بعضی از مواقع باعث هنگ کردن سیستم عامل می شود .

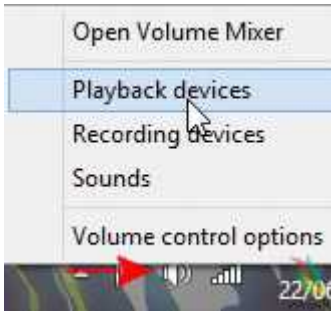
"Windows Audio Device Graph Isolation" نمودار تفکیک صدای ویندوز

علت پردازش بالای Windows Audio Device Graph Isolation چیست ؟

1. درایور صدا یا خیلی قدیمی می باشد یا نسخه جدید با سیستم عامل سازگار نمی باشد
2. افکت های صوتی زیادی در حال فعالیت هستند. (مثلا استفاده از افکتهای BBE در Jetaudio)
3. نصب کدک های زیاد بر روی ویندوز می تواند باعث بروز چنین مشکلی شود .

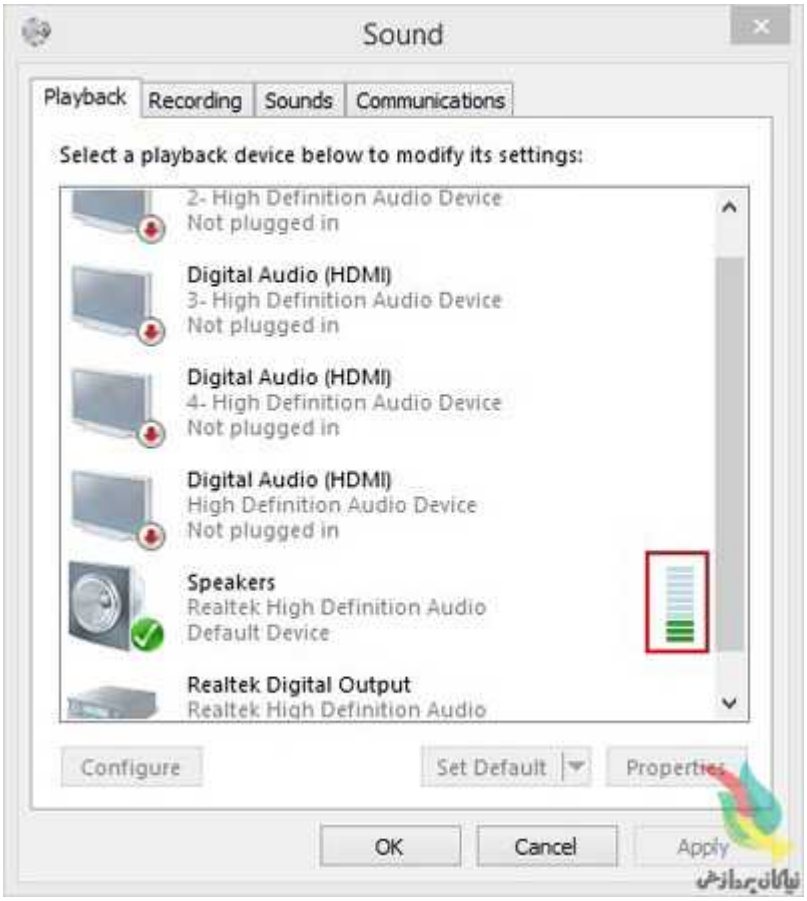
۴ر در بعضی مواقع اسپیکرهای قوی وقتی توانشون از کارت صدای ویندوز بالاتر باشه و نیاز به پردازش بیشتری هم داشته باشه این مشکل بوجود می آید .

بر روی آیکون صدا در نوار وظیفه کلیک راست کرده و گزینه Playback Devices را انتخاب کنید .

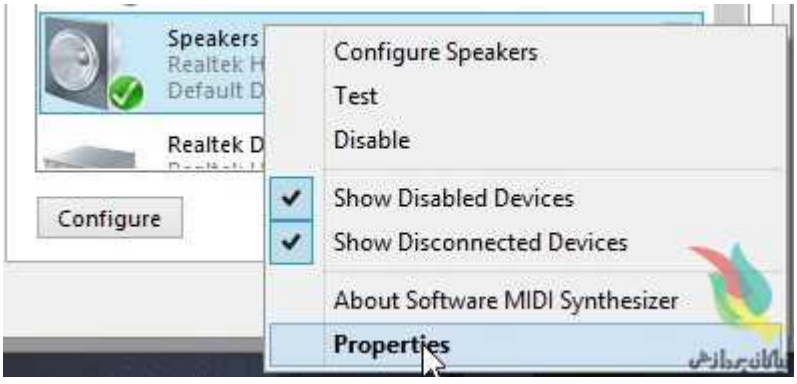


پنجره بعدی تنظیمات مربوط به صدا می باشد . در صورتیکه گزینه های

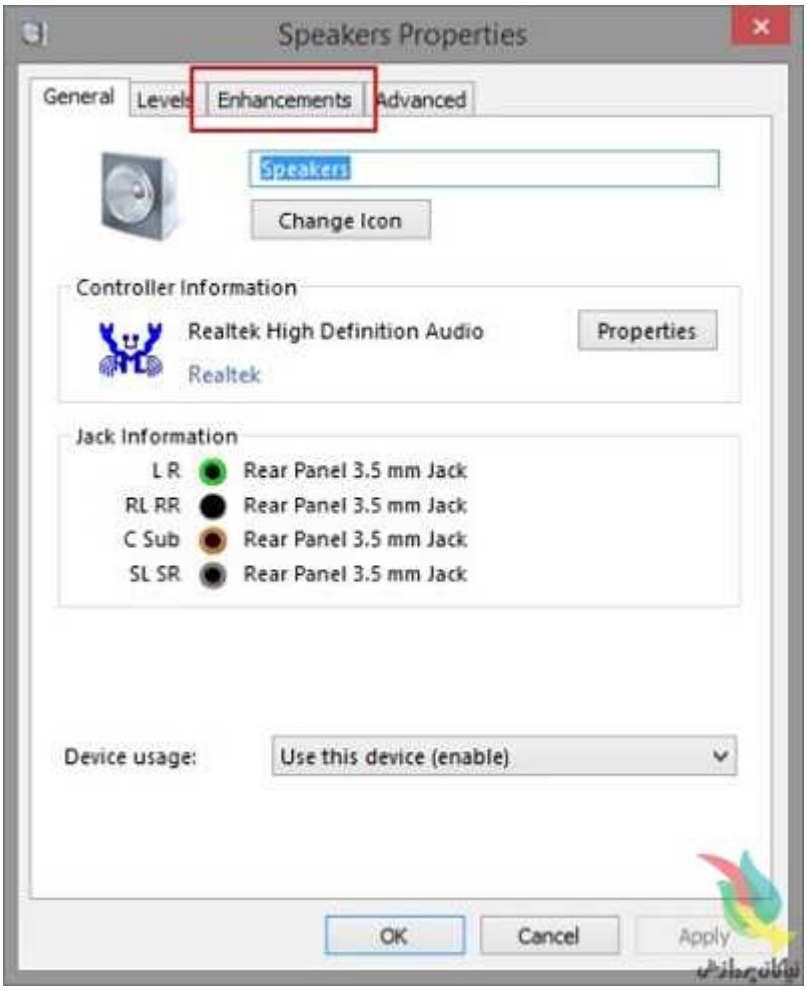
زیادی در این پنجره مشاهده می کنید جای نگرانی وجود ندارد چون به صورت پیش فرض آیکون اسپیکر با رنگ سبز مشخص شده است .



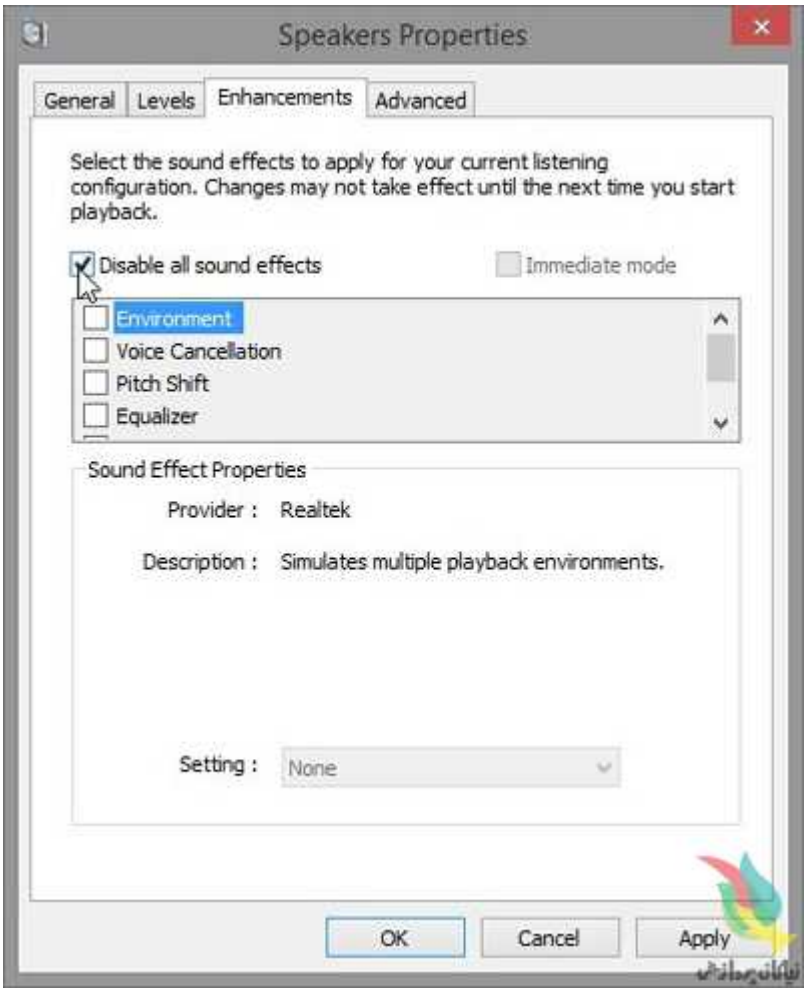
بر روی آیکون کارت صدا کلیک راست کرده و گزینه "Properties" را انتخاب کنید .



به سربرگ / تب "Enhancements" بروید . یا بر روی تب "Enhancements" کلیک کنید .



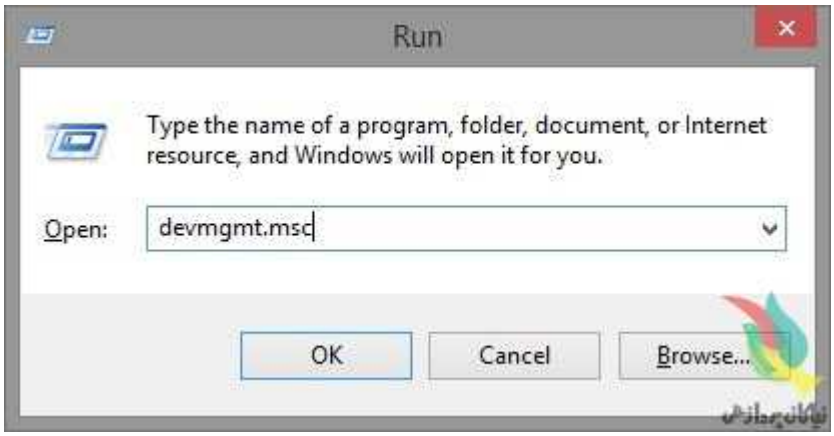
برای غیر فعال کردن جلوه های صوتی صدا بالای صفحه بر روی چک باکس گزینه disable all sound effects کلیک کنید تا غیر فعال شود .



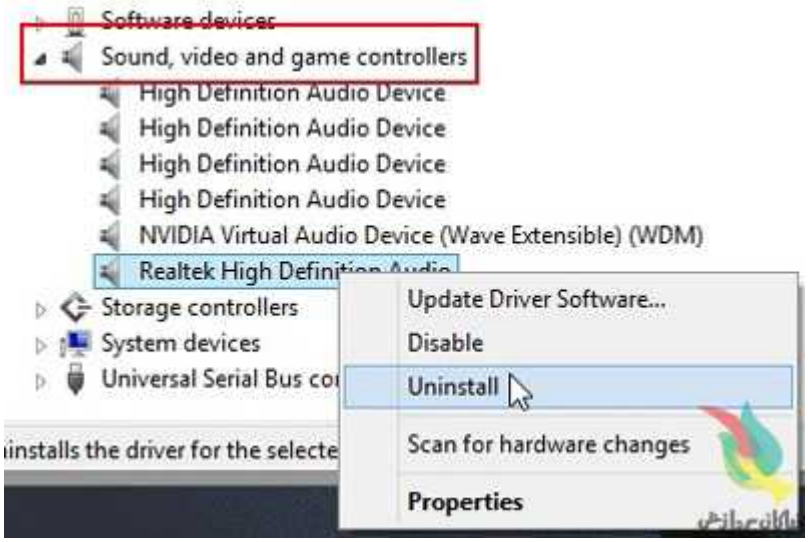
نصب مجدد درایور صدا

برای رفع مشکل پردازش صدا بهتر است درایور کارت صدا هم بررسی کنید . ابتدا باید درایور صدا را حذف کنیم و از دوباره نصب کنیم . قبل از انجام اینکار بهتر است آخرین نسخه درایور کارت صدا را دانلود کنید سپس با استفاده از ادامه این آموزش درایور صدا را حذف و از دوباره نصب کنید .

کلیدهای ترکیبی "Windows Key + R" را همزمان بفشارید سپس دستور devmgmt.msc را تایپ کرده و بر روی کلید اینتر کلیک کنید .



بر روی درایور کارت صدا "Sound, video and game controllers", کلیک راست کرده و گزینه Uninstall را انتخاب کنید .



پنجره باز شده را با انتخاب گزینه OK تایید کنید .



فعال کردن حالت تبلت در ویندوز ۱۰

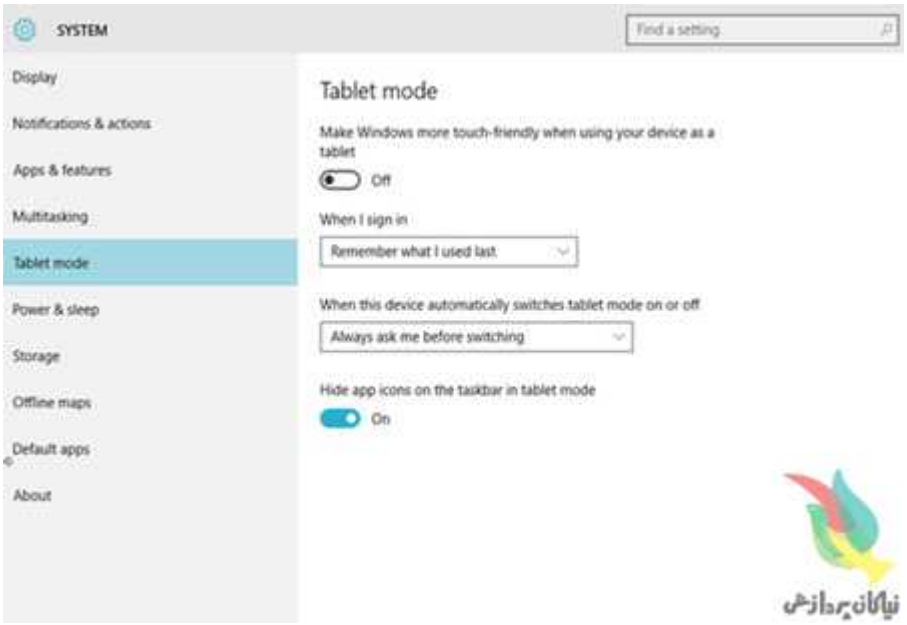


قابلیت کانتینیوم ویندوز ۱۰، به صورت پویا زمانی که از یک صفحه‌ی لمسی استفاده کنید یا زمانی که صفحه کلیدی را به تبلت یا رایانه‌ی هیبریدی متصل یا جدا می‌کنید، از دسکتاپ سنتی به رابط کاربری مدرن جابه‌جا می‌شود. اما اگر از رایانه‌ی شخصی دسکتاپ استفاده می‌کنید و خواستار نرم‌افزارهای تمام صفحه و صفحه‌ی شروع با کاشی‌های زنده هستید، باید دکمه‌ی Tablet Mode را بزنید.



اکشن‌سنتر جدید ویندوز ۱۰ را با کلیک بر روی آیکن موجود در سمت راست نوار وظیفه باز کنید و دکمه‌ی Tablet Mode را بزنید. با این کار، همه چیز از دسکتاپ حذف شده و بین آیکنهای منوی استارت،

کورتانا و تسک ویو فاصله می‌افتد. حالا در صورت باز بودن پنجره‌ی نرم‌افزار خاصی، برای نمایش نرم‌افزارهای تمام صفحه و صفحه‌ی شروع، دکمه‌ی استارت را بفشارید. اگر خواستار نمایان کردن آیکن نرم‌افزارهای پین شده به نوار وظیفه هستید، در ادامه‌ی مقاله به طریقه‌ی نمایش آن‌ها اشاره می‌کنیم.



سفارشی سازی حالت تبلت

زمانی که در حال استفاده از دستگاه هیبریدی هستید، ویندوز ۱۰ به طور هوشمندانه بین حالت سنتی و مدرن جابه‌جا می‌شود. اما در صورتی که همیشه قصد استفاده از حالت تبلت را ندارید، می‌توانید نحوه‌ی اجرای ویژگی کانتینیوم را هم به وسیله‌ی ویندوز سفارشی بسازید!

به سادگی عبارت Tablet Mode را جستجو کنید و Tablet Mode Settings را از میان گزینه‌های نمایان شده، انتخاب کنید. در این بخش از تنظیمات، شما قادر به فعال کردن حالت تبلت و تعیین نحوه‌ی جابه‌جا شدن به این حالت از طریق بخش When this device Automatically switches tablet mod on or off هستید. شما همچنین می‌توانید در صورت تمایل، با غیرفعال کردن گزینه‌ی Hide app icons on the taskbar in tablet mod، از مخفی شدن آیکنهای نوار وظیفه هنگام جابه‌جا شدن به حالت تبلت جلوگیری کنید. به علاوه، می‌توانید نحوه‌ی راه‌اندازی سیستم با حالت تبلت و دسکتاپ را هم از طریق When I sign in موجود بخش یاد شده، تنظیم کنید.

خاموش و روشن‌های مک



انجام برخی کارها در سیستم های عامل مختلف جزو امور عادی به‌شمار نمی‌رود، اما در برخی موارد ممکن است اطلاعات ارزشمندی را در اختیار شما قرار دهد.



یکی از این کارها، اطلاع یافتن از مدت زمانی است که رایانه شما روشن بوده یا بررسی تاریخچه زمان‌هایی که رایانه ری‌استارت شده یا خاموش شده است. گرچه دانستن این اطلاعات برای یک کاربر عادی در شرایط طبیعی ضرورتی ندارد، اما همین اطلاعات در بررسی مشکلات رایانه یا رفع عیوب احتمالی مشاهده شده در آن می‌تواند بسیار موثر و ضروری باشد.

دوست دارید بدانید رمزگشایی جعبه سیاه رایانه در سیستم‌عامل مک چگونه است؟ با استفاده از این ترفند به روش‌های مختلفی می‌توانید به این اطلاعات دسترسی یابید:

روش اول (مدت روشن بودن رایانه)

در این روش از ابزار System Information کمک می‌گیریم. برای اجرای این ابزار از نوار منوی اصلی روی آیکون اپل کلیک کرده و کلید Option را فشار دهید تا گزینه About This Mac به System Information تغییر کند سپس روی گزینه System Information کلیک کنید.

از ستون سمت چپ روی Software کلیک کرده و مدت زمان به‌نمایش درآمده (مدت روشن بودن رایانه در بوت فعلی) را در مقابل عبارت Time since boot در ستون سمت راست مشاهده کنید.

روش دوم (مدت روشن بودن رایانه)

ابزار ترمینال را اجرا کرده و فرمان uptime را در آن وارد کنید و کلید اینتر را فشار دهید.

با اجرای این فرمان، به ترتیب زمان فعلی رایانه، مدت زمان روشن بودن رایانه، تعداد پنجره‌های ترمینال در حال اجرا و میانگین پردازش‌های موجود روی سیستم‌عامل در بازه‌های زمانی ۱، ۵ و ۱۵ دقیقه اخیر به شما نمایش داده می‌شود.

روش سوم (تاریخچه ری‌استارت و خاموشی‌ها)

ترمینال را اجرا کرده و یکی از فرمان‌های last reboot یا last shutdown را در آن وارد کرده کلید اینتر را فشار دهید.

با اجرای هریک از این فرمان‌ها، تاریخچه کاملی از زمان کل ری‌استارت و خاموش شدن‌های رایانه در اختیار شما قرار می‌گیرد. این تاریخچه از ابتدای نصب سیستم‌عامل روی رایانه شما قابل مشاهده است و اگر می‌خواهید بدانید چند وقت پیش سیستم‌عامل رایانه را نصب کرده‌اید کافی است آخرین ردیف موجود را مشاهده کنید.

بیدارباش ویندوز بدون رمز



یکی از کارهایی که به‌عنوان عادت‌های خوب برای یک کاربر ویندوزی به‌شمار می‌رود، فعال‌سازی قابلیت Sleep در شرایطی است که برای مدتی از رایانه استفاده نمی‌کنید.



با استفاده از این قابلیت نه‌تنها در مصرف برق صرفه‌جویی می‌شود بلکه عمر مفید سخت‌افزار رایانه نیز افزایش می‌یابد. این قابلیت برای بسیاری از کاربران سودمند است و در بسیاری از موارد نیز کاربران برای حفاظت از اطلاعات ذخیره شده در رایانه خود، یک رمز عبور برای ورود به ویندوز اختصاص می‌دهند.

این رمز علاوه بر روشن شدن اولیه رایانه، هنگام خروج از حالت Sleep نیز درخواست می‌شود و ممکن است برخی کاربران هنگام ترک رایانه خود در محیطی حضور داشته باشند که دسترسی هیچ کاربر غیرمجازی به رایانه امکان‌پذیر نباشد.

در این شرایط حتی اگر دسترسی به رایانه بدون رمز نیز امکان‌پذیر باشد، امنیت کاربر در خطر نخواهد بود و برای جلوگیری از اتلاف وقت برای تایپ کردن رمز، هنگام خروج از حالت Sleep می‌توان با یک ترفند ساده این قابلیت را غیرفعال کرد.

به این ترتیب رایانه شما هنگام روشن شدن اولیه، نیازمند رمز عبور خواهد بود و در ادامه هنگامی که قابلیت Sleep فعال می‌شود و قصد

خروج از این حالت را داشته باشید هیچ رمزی از شما درخواست نخواهد شد.

به بخش Settings در ویندوز وارد شوید. (می‌توانید عبارت Settings را در کادر جست‌وجوی ویندوز ۱۰ وارد کنید و روی نتیجه یافت شده با همین عنوان کلیک کنید)

گزینه Accounts را انتخاب کرده و به بخش Sign-in options وارد شوید.

به بخش Require sign-in رفته و از منوی پایین افتادنی گزینه Never را انتخاب کنید.

مراحل کار به اتمام رسیده و از حالا به بعد هنگام خروج از حالت Sleep رمز عبوری از شما درخواست نمی‌شود.

فهرست الفبایی منوی استارت ویندوز ۱۰



ویندوز ۱۰ برای جبران شکست مایکروسافت در ارائه ویندوز ۸ و ۸٫۱، تغییرات زیادی را در خود جای داد که یکی از مهم‌ترین این تغییرات ترکیبی از سنت و مدرنیته در منوی استارت آن است.



در این نسخه از ویندوز مایکروسافت تلاش کرده با حفظ کاشی‌های زنده در کنار منوی استارت کلاسیک ویندوز ۷ و پیش از آن، به‌روز بودن را در کنار عادت‌های کاربران قدیمی خود یکجا به کاربران ارائه کند.

شاید در نگاه اول، منوی استارت در ویندوز ۱۰ فقط همین تغییر را داشته باشد، اما اگر کمی بیشتر به آن توجه کنید متوجه تغییرات جزئی دیگری نیز خواهید شد که در مواردی می‌تواند سرعت استفاده از ابزارهای موجود در این منو را افزایش دهد. یکی از این تغییرات که کمتر کاربری به آن توجه می‌کند، مجهز بودن به فهرست الفبایی برای پرش سریع میان گزینه‌های موجود طبق حروف الفبای موردنظر است.

برای دسترسی به این فهرست کافی است از روش زیر کمک بگیرید:

روی منوی استارت کلیک کنید.

کمی منو را به سمت پایین اسکرول کنید تا فهرست اپلیکیشن‌ها به ترتیب حروف الفبا نمایان شود.

بسیاری از کاربران در این مرحله فکر می‌کنند نمایش حروف الفبا فقط برای تفکیک بخش‌ها از یکدیگر است، در صورتی‌که می‌توانید روی هریک از حروف به‌نمایش درآمده در منو کلیک کنید تا فهرست الفبایی برای شما نمایش داده شود.

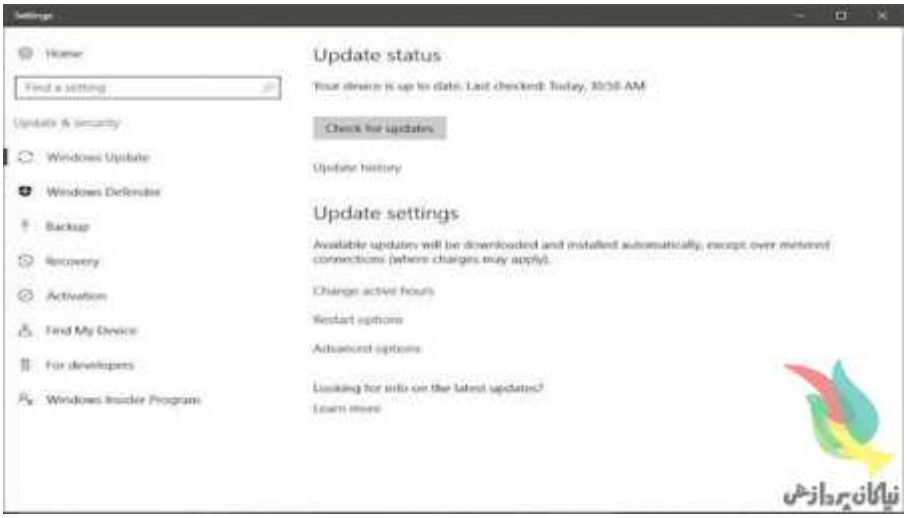
پس از نمایش فهرست الفبا روی حرف موردنظر کلیک کنید تا به مجموعه اپلیکیشن‌هایی که عنوانشان با حرف موردنظر آغاز می‌شود، پرش کنید.

از حالا به بعد به همین سادگی می‌توانید اپلیکیشن‌هایی را که با حرف X شروع می‌شوند نیز مشاهده کنید و نیازی به اسکرول کردن فهرست گزینه‌های موجود در منو برای رسیدن به انتهای فهرست و حرف

X نخواهید داشت.

غیرفعالسازی بهروز رسانی ویندوز ۱۰



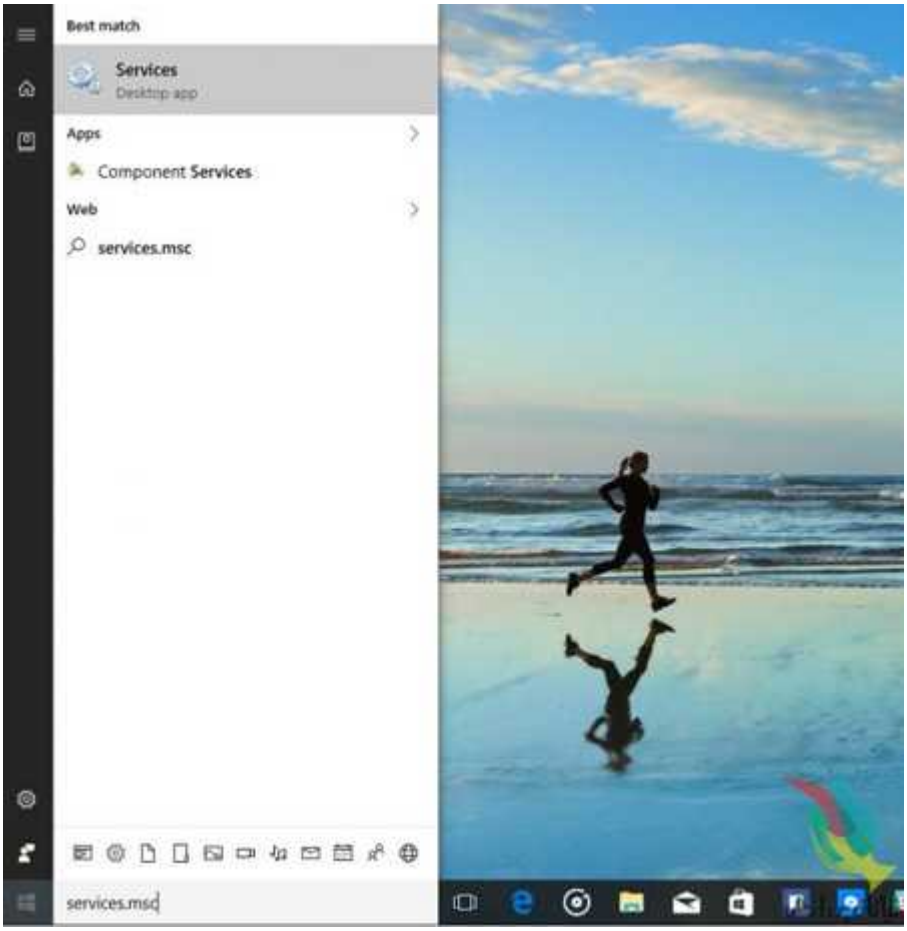


یکی از سرویسهای ویندوز ۱۰ به روزرسانیهای اتوماتیک است که به حالت پیشفرض روی کامپیوتر شما فعال است و هر از چند گاهی سیستمعامل را آپدیت میکند؛ هنگامی که سیستم آنلاین به روزسانی میشود دیگر احتیاجی نیست که نگران از دست رفتن درایوهای دستگاه باشید. ویندوز اتوماتیکوار آپدیتهای لازم را اگر در دسترس باشند نصب میکند، اما بعضی از کاربران، به روزرسانی هر چند وقت یکبار ویندوز را اتلاف وقت یا بیهوده میدانند.

در ویندوز ۸.۱ و ورژنهای قبلی امکان غیر فعال کردن آپدیتها در اختیار کاربر بود؛ اما متاسفانه در ویندوز ۱۰ مایکروسافت هیچ گزینهایی را برای غیر فعال کردن آپدیتها برای کاربران عمومی قرار

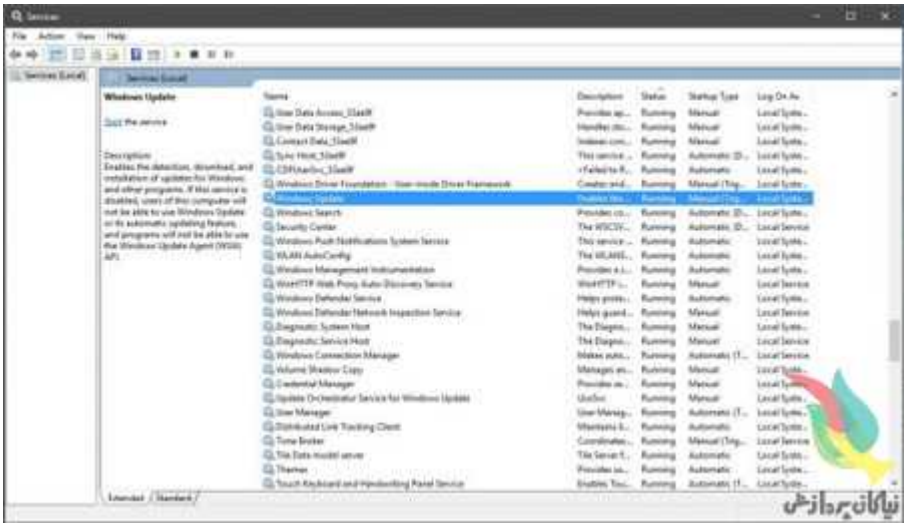
نداده ولی ما به شما راهی را پیشنهاد می‌دهیم که می‌توان با استفاده از آن به روزرسانی ویندوزتان را خاموش کنید.

قدم اول: در قسمت جستجو عبارت service.msc را سرچ کرده و آن را باز کنید.



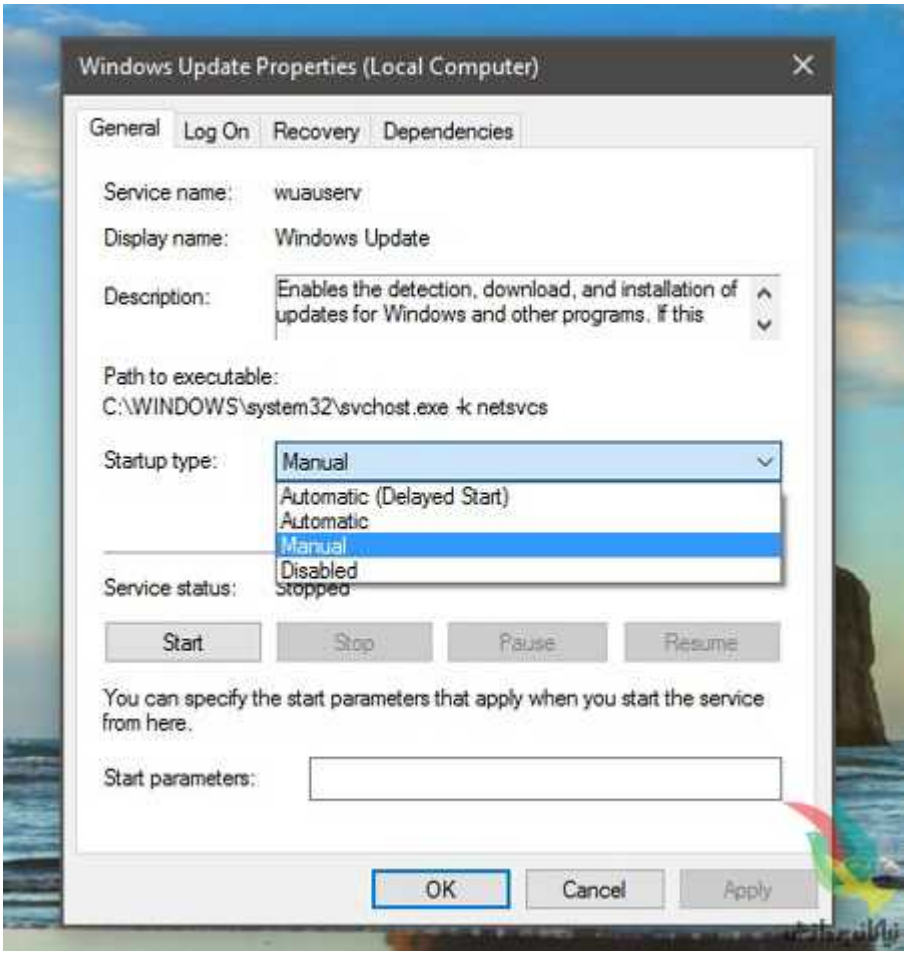
غیر فعالسازی به‌روز رسانی ویندوز

قدم دوم: از لیست باز شده Windows Update را انتخاب کنید.



غیر فعال کردن آپدیت ویندوز ۱۰

قدم سوم: دو بار روی گزینه انتخاب شده کلیک کنید و در پنجره باز شده در تب General همانند شکل زیر گزینه Disabled در قسمت Start type را انتخاب کنید.



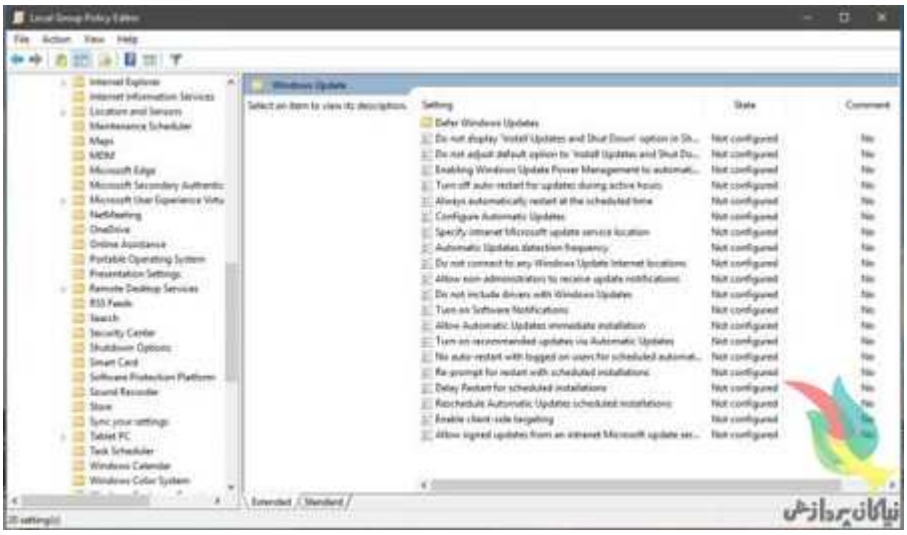
آپدیت سیستم‌عامل ویندوز ۱۰

قدم چهارم: اول گزینه Apply و بعد از آن Ok را بزنید.

از این مرحله به بعد دیگر ویندوز شما اتوماتیکوار شروع به آپدیت شدن نمی‌کند تا موقعی که خودتان بخواهید این کار را انجام بدهید؛ اگر بخواهید به حالت قبل برگردید باید گزینه Disabled را با Automatic جایگزین کنید و یک بار سیستم را خاموش و روشن کنید.

اگر کامپیوتر شما به شبکه متصل باشد و تیمی از سیستم عامل استفاده می‌کنید، ممکن است روش بالا برایتان جواب ندهد، پس باید با فرد پشتیبان فناوری اطلاعات شرکت صحبت کنید و اگر خودتان ادمین باشید می‌توانید با استفاده از روش زیر به روزرسانی را غیرفعال کنید.

قدم اول: در قسمت جستجو عبارت Edit group policy را تایپ کرده و آن را باز کنید.



قدم دوم: در پوشه باز شده این مسیر را بروید: Computer Configuration>Administrative Templates>Windows Components>Windows Update.

قدم سوم: ادامه کار همانند قدم سوم و چهارم در روش قبلی است.

منبع:digiro.ir