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.

تصـــویری گویـــا از علـــل 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.

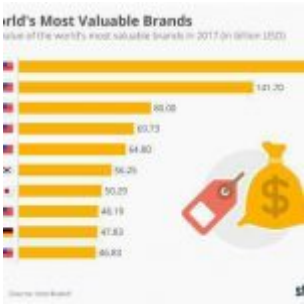
از برنامه های دم دستی و تجاری مثل ESET یا Nodو مانند اینها کاری بر نمیاد.

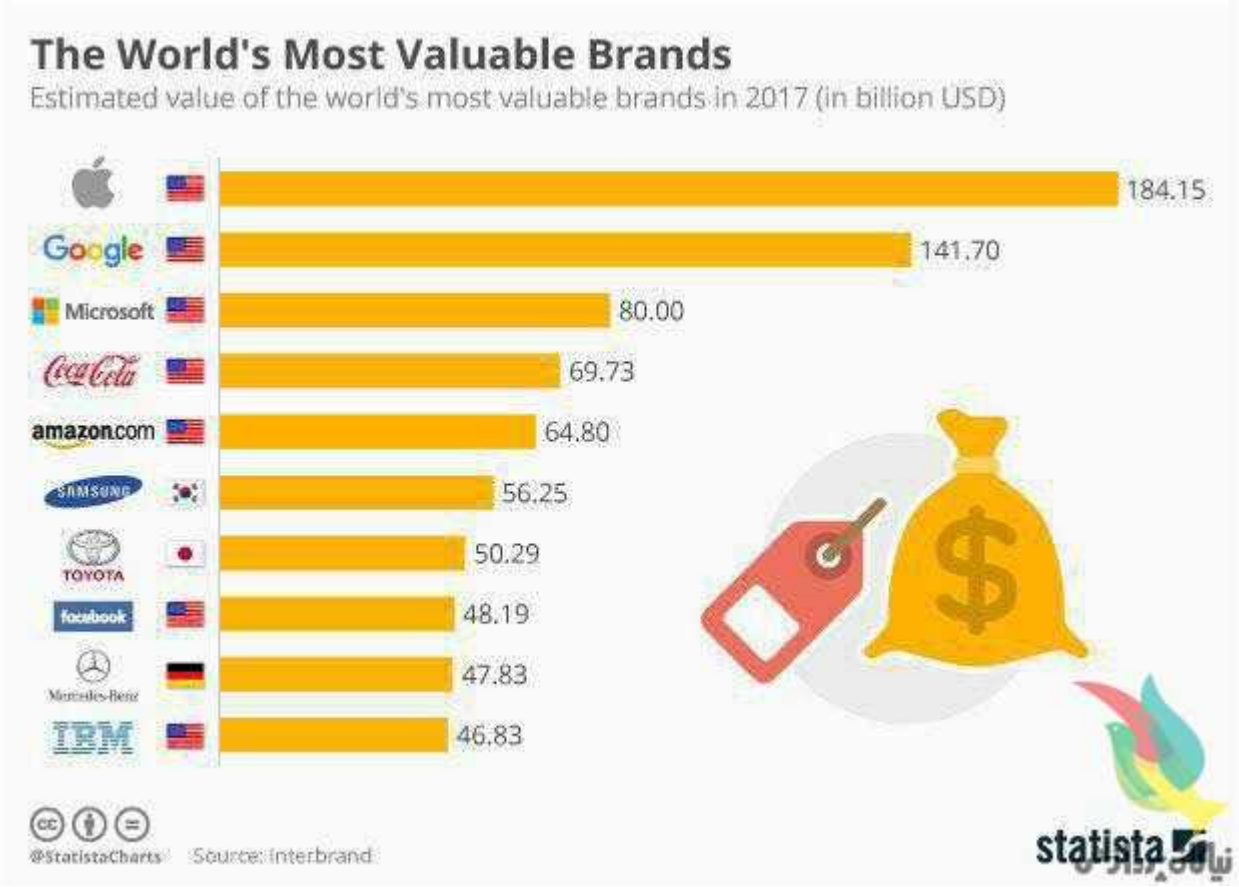
تفاوت اپل و گوگل در یک آمار ساده

تفاوت اپل و گوگل در یک آمار ساده

هزینه تبلیغات
اپل:۱.۸ میلیارد
گوگل:۳.۲ میلیارد
درآمد
اپل:۲۳۳ میلیارد
گوگل:۶۸ میلیارد
ارزش
اپل:۱۵۴ میلیارد
گوگل:۸۲ میلیارد

ارزشمندترین برندهای سال ۲۰۱۷ را بشناسیم!





۱. اپل
۲. گوگل
۳. مایکروسافت
۴. کوکاکولا
۵. آماوزن
۶. سامسونگ

۷. تویوتا
۸. فیس بوک
۹. مرسدس بنز
۱۰. آی بی ام

چگونه از ریپورت اینستاگرام خارج شویم؟

معمولاً در شبکه‌های اجتماعی قوانینی وجود دارد که کاربران باید این قوانین را رعایت کنند. اینستاگرام نیز از این قاعده مستثنی نیست و قوانین و مقرراتی دارد که کاربران اینستاگرام موظف به رعایت این قوانین می‌باشند.

برای نمونه شما نمی‌توانید از تصاویر نژادپرستانه در پست‌های اینستاگرام خود استفاده کنید و یا پست‌های دیگران را به نام خود به اشتراک بگذارید! در سایت اینستاگرام در قسمت TERMS این قوانین

بیان شده است. حال ریپورت اینستاگرام چیست؟

اگر کاربران قوانین اینستاگرام رعایت نکنند، این اقدام می‌تواند باعث حذف اکانت اینستاگرام آنها شود.

کاربران در اینستاگرام می‌توانند عمل خلاف قوانین دیگر کاربران را گزارش دهند، که به این عمل، ریپورت کردن گفته می‌شود. این ریپورت کردن می‌تواند شامل کاربر، پست، تصویر و یا کامنتی باشد. این موارد شامل ریپورت می شوند:

انتشار تصویر یا کامنت تبلیغاتی و اسپم

انتشار پست و تصاویر دیگران به نام خود

عدم رعایت قانون کپی رایت

انتشار تصاویر و کامنت‌های غیر اخلاقی

پست‌ها و کامنت‌هایی شامل خودکشی، تهدید و آزار و استفاده از مواد مخدر

این نکته را در نظر داشته باشید که اگر ریپورت‌های غیر واقعی ارسال شود، منجر به بسته شدن آن اکانت نمی‌شود.

رفع مشکل ریپورت اینستاگرام و بلاک شدن در اینستاگرام

در صورتی که برای کامنت گذاشتن، لایک کردن و فالو کردن و … با مشکل مواجه شده‌اید، احتمالاً با مشکل ریپورت و بلاک شدن مواجه شده‌اید. بلاک شدن یک کاربر ممکن است توسط کاربران صورت گرفته باشد و یا توسط اینستاگرام کاربری بلاک شده باشد.

رفع ریپورت اینستاگرام و بلاک شدن توسط اینستاگرام

اگر برای کامنت گذاشتن در اینستاگرام با مشکل مواجه شده‌اید، احتمالاً در یک بازه زمانی بیش از حد مجاز کامنت ارسال کرده‌اید، این مشکل پس از چند ساعت رفع می‌شود. اما اگر با مشکل لایک کردن مواجه شده‌اید، در یک بازه زمانی بیش از اندازه لایک کرده‌اید.

بلاک شدن شما برای فالو کردن، به این معنی می‌باشد که شما یا در یک بازه زمانی بیش از اندازه فالو کرده‌اید و یا بیش از ۷۵۰۰ فالو کرده‌اید. رفع این نوع از بلاک شدن توسط اینستاگرام ممکن است تا یک

ماه طول بکشد.

برای رفع مشکل بلاک شدن توسط اینستاگرام راهکارهای زیر را انجام دهید:

راهکار اول برای رفع بلاک شدن توسط اینستاگرام:

یکی از راهکارهای معمول، این است که از فالوورهای خود بخواهید تا برای شما کامنت انگلیسی ارسال کنند. در واقع با این روش به اینستاگرام ثابت می‌کنید که شما اسپم نیستید! به این منظور می‌توانید از تصاویر زیر به همراه یک پیام متنی استفاده کنید:

راهکار دوم برای رفع بلاک شدن توسط اینستاگرام:

راهکار دیگربرای رفع ریپورت اینستاگرام ، تغییر ایمیل اکانت می‌باشد. به این منظور وارد پروفایل خود شوید و گزینه Edit your profile را انتخاب نمایید. حال در قسمت Private information می‌توانید شماره تلفن و ایمیل خود را ویرایش کنید. بعد از تغییر ایمیل یا شماره تلفن، پیامی حاوی یک لینک ارسال می‌شود که باید بر روی آن کلیک کنید.

چگونه بفهمیم چه کاربری ما را ریپورت و بلاک کرده است؟

قبل از هرچیز باید متوجه شوید که چه کسی شما را بلاک کرده است، اما اینستاگرام اجازه نمی‌دهد شما به طور مستقیم چک کنید چه کسی شما را آنفالو و یا بلاک کرده است.

اگر دیگر نمی‌توانید پست‌های اکانت کاربری را مشاهده کنید، این احتمال وجود دارد که آن شخص شما را آنفالو و یا بلاک کرده باشد.

یکی از ترفندهایی که می‌توانید بفهمید چه کسی شما را بلاک کرده است، سرچ اکانت آن کاربر می‌باشد. به این منظور اگر به کاربری شک دارید که شما را بلاک کرده باشد، باید در صفحه جستجوی اینستاگرام، نام اکانت آن کاربر را وارد کنید، در صورتی که اسم او برای شما نمایش داده نمی‌شود، احتمالاً آن کاربر شما را بلاک کرده است.

اگر می‌توانید وارد صفحه اینستاگرام کاربر شوید اما وقتی او را فالو می‌کنید، جزء فالوورهای او نمی‌شوید و همچنان دکمه Follow را مشاهده می‌کنید، یعنی توسط او بلاک شده‌اید.

همچنین اگر دیگر اسم او جزء فالوویینگ‌های شما نیست، بازهم می توان احتمال داد توسط آن کاربر آنفالو و یا بلاک شده‌اید.

همچنین اگر با اکانت جدید می‌توانید آن کاربر را فالو کنید ولی با اکانت فعلی خود نمی‌توانید، یعنی آن اکانت شما بلاک شده است.

لوگوی گوگل را به دلخواه تغییر نام دهید.

گوگل یکی از پرکاربردترین مرورگرها در بین کاربران وب است، یکی از قابلیت‌های این مرورگر تغییر نام آن به دلخواه شماست.

لوگوی گوگل را همیشه با رنگ های مختلف دیده اید و گاه به مناسبت‌های گوناگون اشکالی متفاوت از لوگوی گوگل برای شما به نمایش گذاشته شده است، ممکن است عده ای تغییر نام لوگوی گوگل را یک قابلیت جذاب و مناسب برای این مرورگر بدانند که می تواند در کنار تمامی قابلیت های گوگل، این مرورگر را در بین کاربران محبوب تر از گذشته کند.

تغییر نام لوگوی با یک ترفند ساده قابل انجام است و شما می توانید پس از انجام مراحل زیر هر بار که گوگل را باز می کنید به جای نام google، عنوانی را که انتخاب کرده اید، ببینید.

برای شروع در مرورگر گوگل عنوان goglogo را تایپ کنید و اینتر را بزنید.

سپس سایتی که به شما معرفی شده است را باز کنید. در قسمت your name کلیک کنید.

نام دلخواه خود را تایپ کرده و اینتر را بزنید.

همانطور که در تصویر زیر مشاهده می کنید صفحه گوگل به نامی که شما انتخاب کرده اید تغییر پیدا کرده است.

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

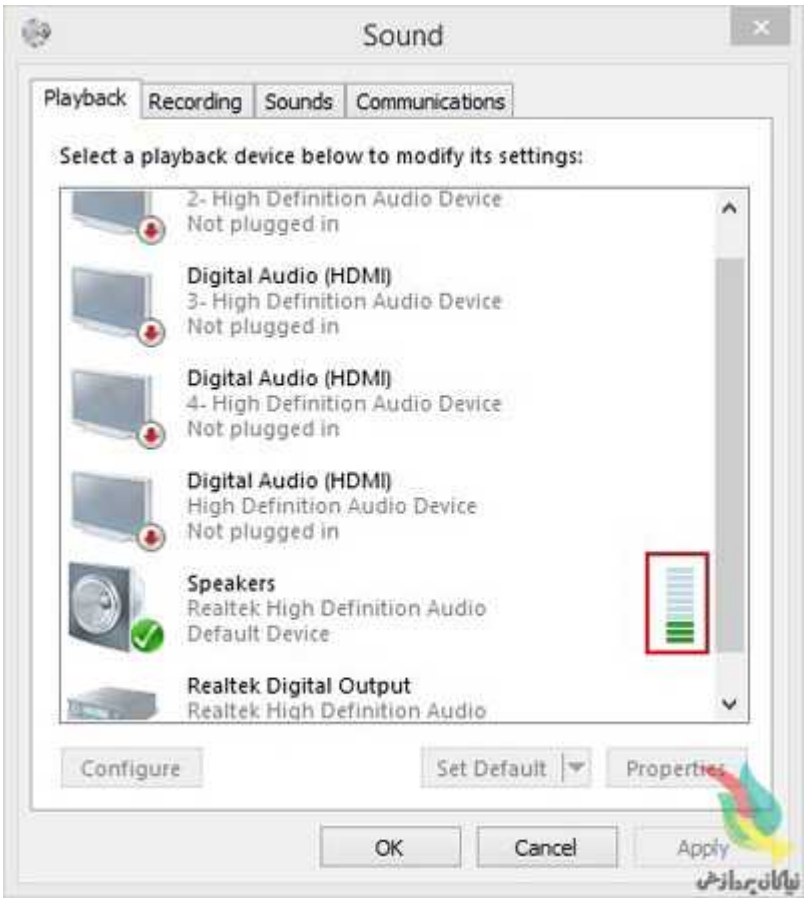
علت پردازش بالای Windows Audio Device Graph Isolation چیست ؟

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 .

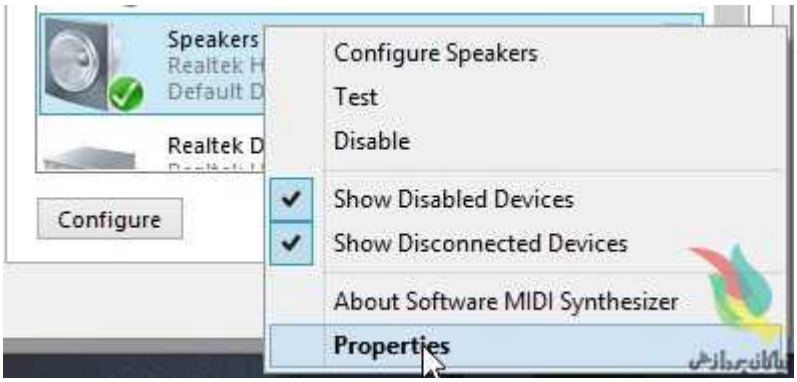
۴ر در بعضی مواقع اسپیکرهای قوی وقتی توانشون از کارت صدای ویندوز بالاتر باشه و نیاز به پردازش بیشتری هم داشته باشه این مشکل بوجود می آید .

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

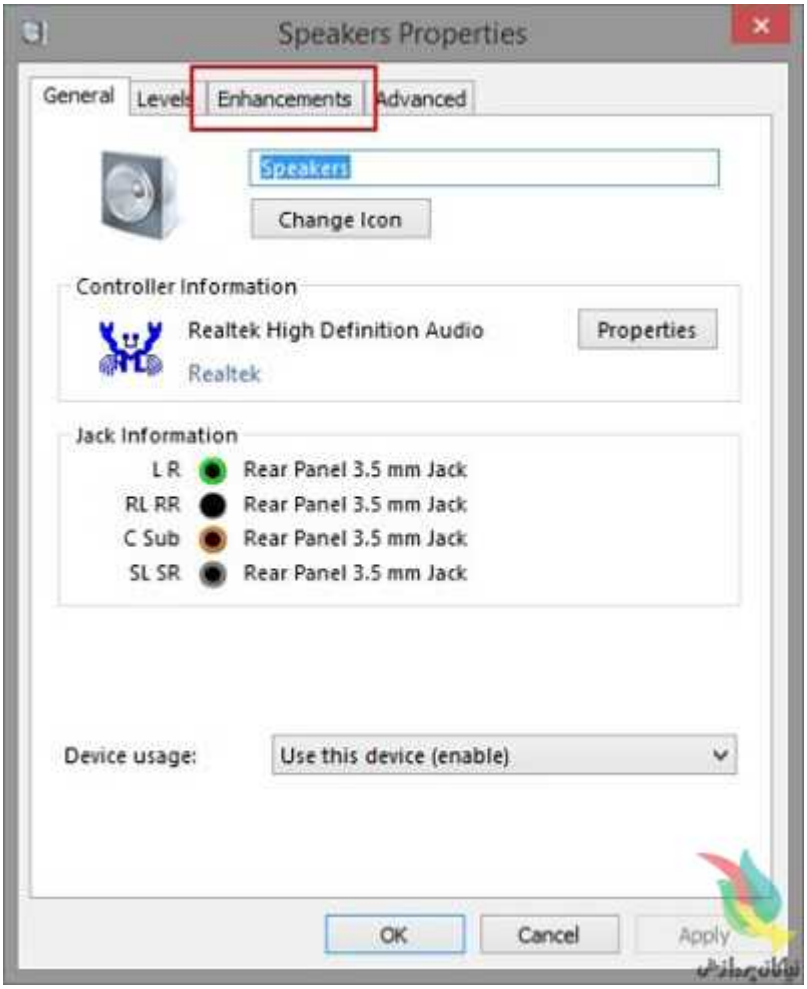
پنجره بعدی تنظیمات مربوط به صدا می باشد . در صورتیکه گزینه های زیادی در این پنجره مشاهده می کنید جای نگرانی وجود ندارد چون به صورت پیش فرض آیکون اسپیکر با رنگ سبز مشخص شده است .



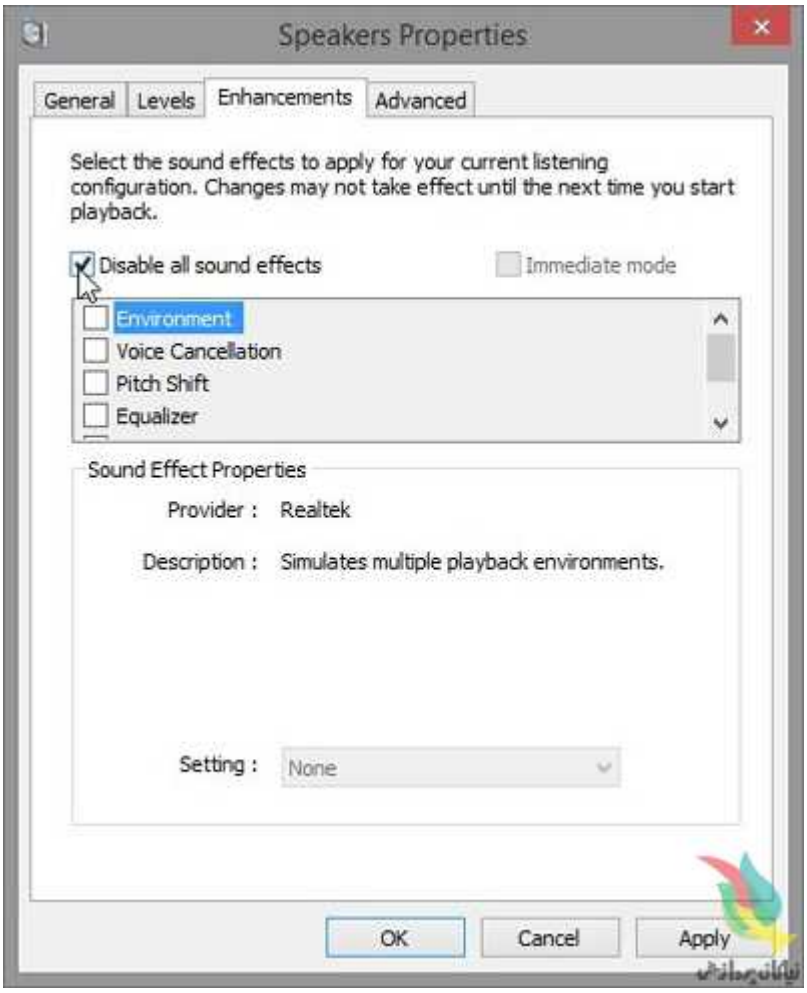
بر روی آیکون کارت صدا کلیک راست کرده و گزینه "Properties" را انتخاب کنید .



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



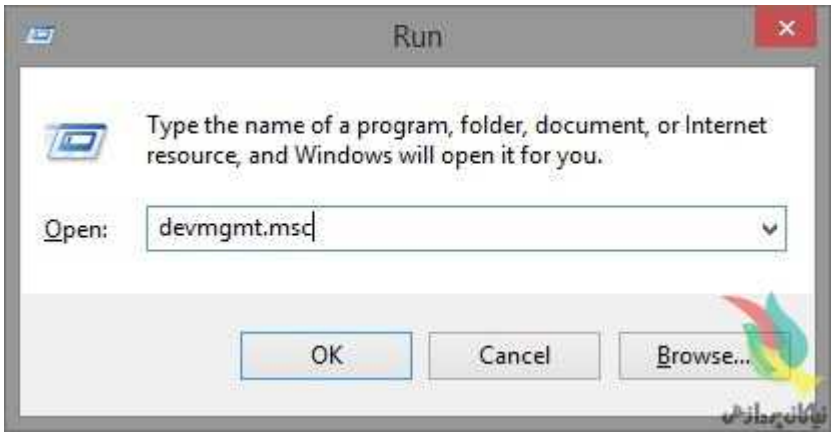
برای غیر فعال کردن جلوه های صوتی صدا بالای صفحه بر روی چک باکس گزینه disable all sound effects کلیک کنید تا غیر فعال شود .



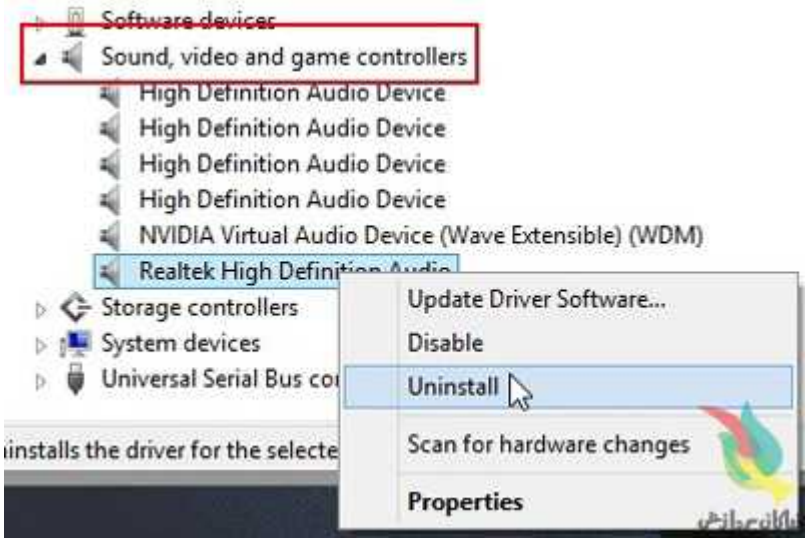
نصب مجدد درایور صدا

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 .



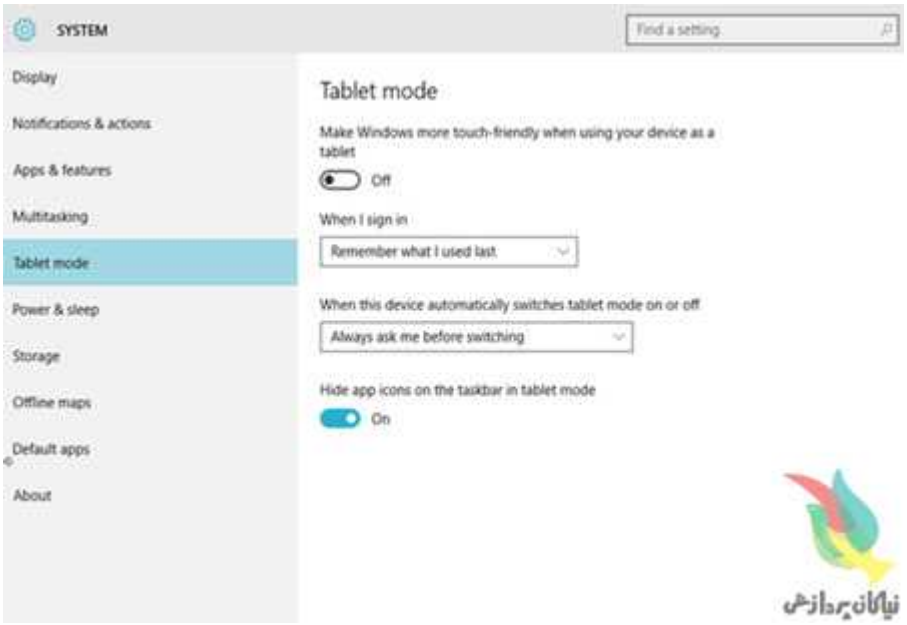
پنجره باز شده را با انتخاب گزینه OK تایید کنید .

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.