ICDL چیست ؟

در بیشتر کشورهای توسعه یافته و صاحب فناوری و در بعضی کشورهای در حال توسعه آموزش علوم کامپیوتری و فراگیری دانش - IT Information Technology جزو برنامه های اصلی مدارس ، دبیرستانها و دانشگاهها به شمار می آید . در ایران نیز برنامه توسعه و کاربردی فناوری ارتباطات و اطلاعات موسوم به (تکفا) مهمترین برنامه دولت در زمینه توسعه ، گسترش و کاربردی ساختن IT در کشور محسوب می شود .

ICDL- International Computer Driving License ICDL گواهینامه ای است بین المللی جهت استفاده از کامپیوتر در حدی که نیازهای مقدماتی و اصلی کاربر را پاسخگو باشد .

حملاتی که به گوشی های هوشمند انجام میشود

تشریح نفوذ به یک دستگاه تلفن همراه

چگونه یک هکر می‌تواند از گوشی شما سو استفاده کند؟

اندروید گوشی هوشمند شما ممکن است مبرا به نظر برسد، اما هنگامی که توسط بدافزارها مورد حمله قرار بگیرد متوجه می‌شوید که اطلاعات شما دیده و جعل می‌شود. شرکت در فعالیت های خودکار اینترنتی خطرناک است، و دزدیدن اطلاعات شخصی شما و حتی سرقت پول شما امکان دارد اتفاق بیافتد.

نظارت

- صدا
- دوربین
- لیست تماس
- موقعیت مکانی
- پیامک‌ها

جعل هویت

- فرستادن پیامک‌های شما
- ارسال پیام‌های ایمیل
- ارسال بر روی شبکه‌ی اجتماعی شما

سرقت اطلاعات

- اطلاعات حساب کاربری
- لیست ارتباطات
- لیست تماس‌ها
- شماره تلفن
- دزدیدن اطلاعات توسط برنامه‌های آسیب‌پذیر
- سرقت شماره سریال دستگاه (IMEI)

زیان مالی

- ارسال پیام نرخ حق بیمه
- دزدیدن شماره تراکنش احراز هویت (TANs)
- اخاذی توسط برنامه‌های مخرب
- شماره تلفن
- آنتی ویروس تقلبی
- برقراری تماس‌های گران‌قیمت

فعالیت‌های خودکار مخرب

- اجرای برنامه‌های هک
- تبلیغات مزاحم
- ارسال پیام نرخ حق بیمه

هزینه ی عنوان شده توسط محافظان اندروید در برابر برنامه های مخرب.

۱۱۳ گوشی هوشمند در امریکا در هر دقیقه گم می‌شود.

۵.۴ میلیون دلار هزینه متوسط نگهداری از یک شعبه اطلاعات در سال ۲۰۱۲ در امریکا بود.

۳۵۰،۰۰۰ ویروس اندرویدی توسط SophosLabs دیده شده‌است.

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.

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

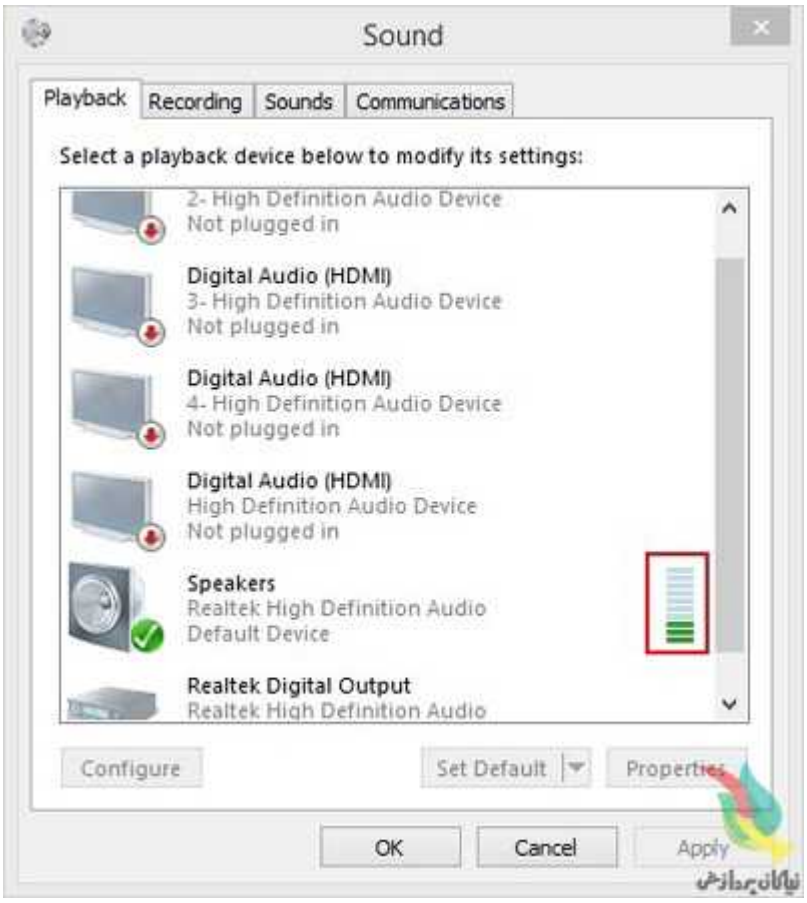
علت پردازش بالای Windows Audio Device Graph Isolation چیست ؟

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 .

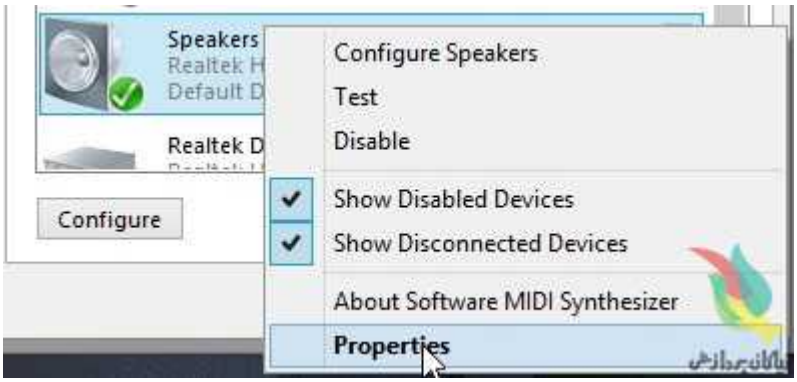
۴ر در بعضی مواقع اسپیکرهای قوی وقتی توانشون از کارت صدای ویندوز بالاتر باشه و نیاز به پردازش بیشتری هم داشته باشه این مشکل بوجود می آید .

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

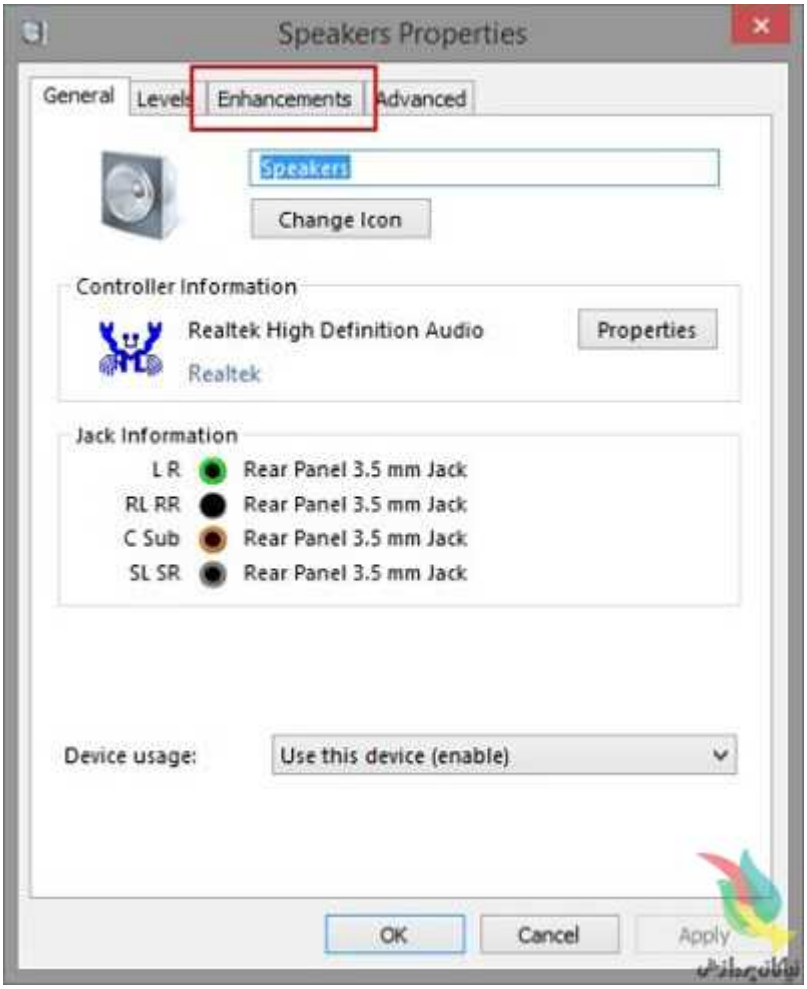
پنجره بعدی تنظیمات مربوط به صدا می باشد . در صورتیکه گزینه های زیادی در این پنجره مشاهده می کنید جای نگرانی وجود ندارد چون به صورت پیش فرض آیکون اسپیکر با رنگ سبز مشخص شده است .



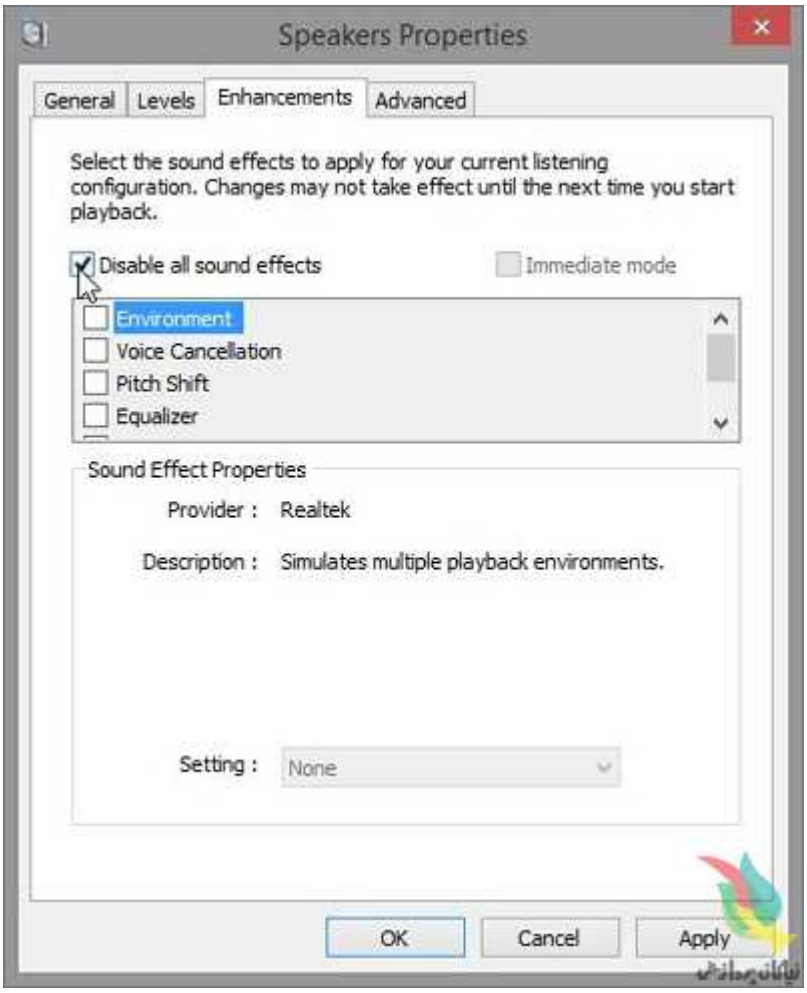
بر روی آیکون کارت صدا کلیک راست کرده و گزینه "Properties" را انتخاب کنید .



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



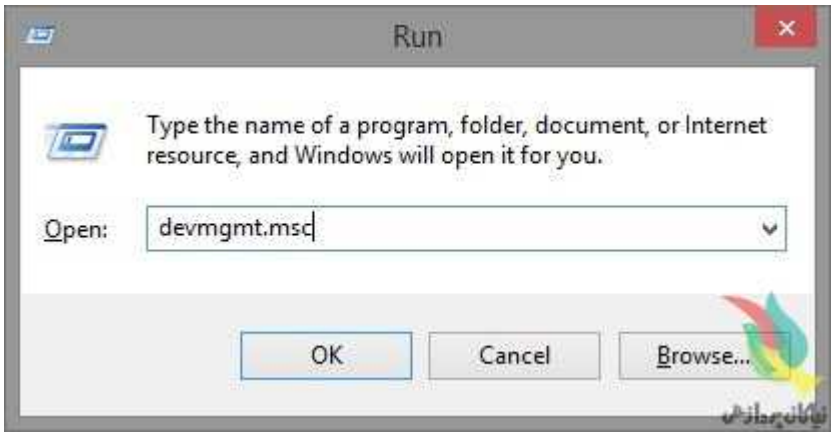
برای غیر فعال کردن جلوه های صوتی صدا بالای صفحه بر روی چک باکس گزینه disable all sound effects کلیک کنید تا غیر فعال شود .



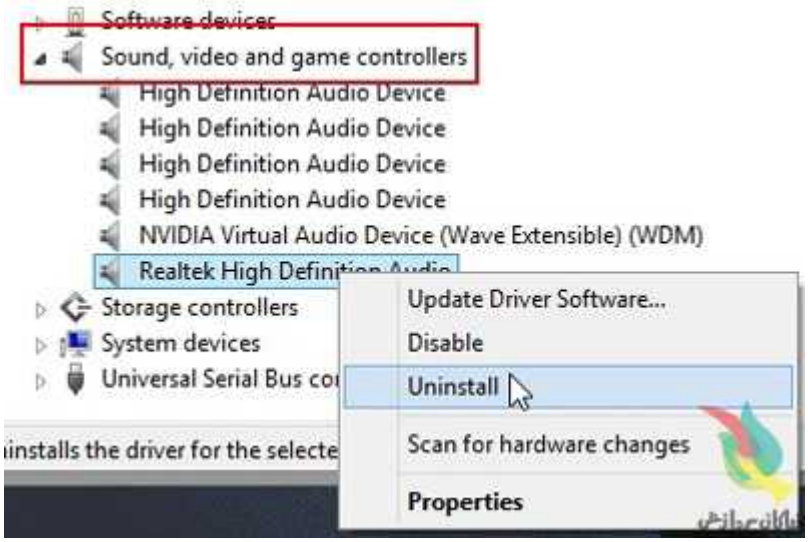
نصب مجدد درایور صدا

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 .

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.

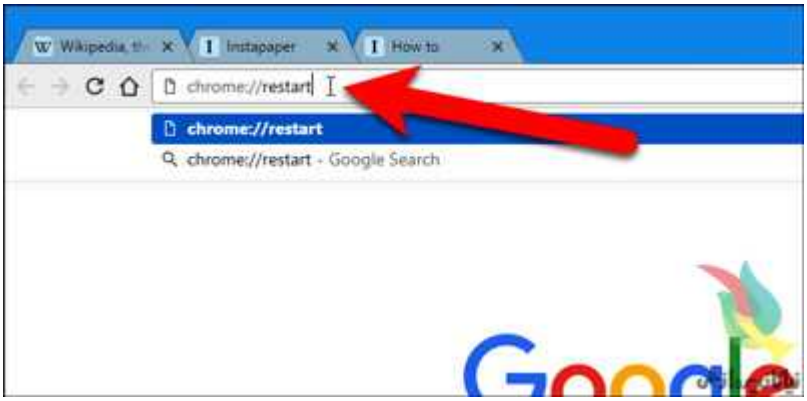
پس از نمایش فهرست الفبا روی حرف موردنظر کلیک کنید تا به مجموعه اپلیکیشن‌هایی که عنوانشان با حرف موردنظر آغاز می‌شود، پرش کنید.

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.

ری‌استارت کروم با میانبر

در شرایط عادی مطمئنا نیازی به ری‌استارت کردن مرورگر (بستن و اجرای مجدد آن) وجود ندارد، اما گاهی ممکن است به هر دلیلی چاره‌ای جز این کار نداشته باشید.



رایج‌ترین روش برای ری‌استارت کردن مرورگر، استفاده از گزینه Close برای بستن آن و در ادامه اجرای مجدد با دوبار کلیک روی آیکون برنامه است. این روش مشکلی ندارد، اما همان‌طور که می‌دانید این صفحه به دوستداران ترفند اختصاص دارد و مرورگر کروم نیز مملو از قابلیت‌های پنهان است.

یکی از این قابلیت‌های پنهان مرورگر، دریافت فرمان‌های خاص با استفاده از نوار آدرس است. به‌عبارت دقیق‌تر مرورگر کروم قادر است مجموعه فرمان‌های مختلفی را با استفاده از نوار آدرس و تایپ عبارت chrome:// در اختیار شما قرار دهد که یکی از این فرمان‌ها نیز

برای ری‌استارت کردن سریع مرورگر کاربرد دارد. این فرمان به‌شرح زیر است:

chrome://restart

اکنون که با این فرمان آشنا شدید می‌توانید به‌صورت یک ترفند برای ری‌استارت کردن سریع مرورگر از آن کمک بگیرید، ولی برای ساده‌تر شدن کار نیز یک ترفند دیگر را با این ترفند ترکیب می‌کنیم تا این فرمان را به فهرست سایت‌های دلخواه در مرورگر اضافه کنیم و بدون نیاز به تایپ فرمان، با یک کلیک روی آن، دستور ذکر شده را فراخوانی کنید. برای استفاده از این ترفند به این روش عمل کنید:

پیش از هر چیز مطمئن شوید نوار بوکمارک‌ها در مرورگر فعال است. برای اطمینان می‌توانید کلیدهای Ctrl+Shift+B را فشار دهید.

حالا به یک سایت دلخواه مراجعه کرده و آیکون آن را از سمت چپ نوار آدرس با روش کشیدن و رها کردن به داخل نوار بوکمارک انتقال دهید.

روی گزینه اضافه شده به نوار بوکمارک کلیک راست ماوس را فشار داده و گزینه Edit را انتخاب کنید.

در بخش Name عنوانی دلخواه همچون «ری‌استارت کروم» را وارد کنید.

در بخش URL نیز عبارت زیر را وارد کنید:

chrome://restart

با کلیک روی Save تغییرات را ذخیره کنید.

از حالا به بعد برای ری‌استارت سریع مرورگر کافی است روی گزینه ایجاد شده در نوار بوکمارک یک‌بار کلیک کنید.