

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 عموماً با پیشنهادهای مهیجی از قبیل برنده شدن در یک مسابقه یا ... می باشد. توجه داشته باشید اینگونه ایمیل ها عموماً از آدرس دوستان شما که هک شده اند برای شما ارسال می شود.

۳ - بر روی لینک های خبرهای مهیج مخصوصاً 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 نکنید. 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 حتماً 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.

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 می‌دهد که این باج‌افزار احتمالاً 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 سیستم‌های کامپیوتری رو هدف قرار دادن ولی میتونن از طریق دستگاههای دیگه و گوشی‌های هوشمند و اینترنت و شبکه‌های 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/فایل‌های تایپی/نقشه‌ها/فایل‌های 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 Nod و مانند اینها کاری بر نیاد.

حذف رمز فایل‌های PDF با کروم



رمزگذاری روی فایل‌های پدیاف به مالک فایل این امکان را می‌دهد از محتوای موجود در فایل حفاظت کند، همچنین گاهی نیز افرادی که این فایل‌ها را منتشر می‌کنند با قرار دادن رمز روی آن سعی می‌کنند نشانی سایت یا هر عبارت دیگری را به کاربران معرفی کنند. ممکن است شما نیز یکی از این فایل‌ها را در اختیار داشته باشید و برای مشاهده محتوای آن نیازمند وارد کردن رمز باشید.



این شرایط مشکل‌ساز در حالت‌های مختلفی برای شما پدیدار می‌شود. اول این‌که شما برای هربار مشاهده محتوای فایل موجود باید رمز آن را وارد کنید و حالت دیگر این‌که ممکن است بخواهید فایل موردنظر را برای فرد دیگری ارسال کنید، اما قصد نداشته باشید فایل رمزگذاری شده را در اختیار آن فرد قرار دهید یا نخواهید او را نیز از عبارت رمز مطلع کنید. (به‌عنوان مثال ممکن است نخواهید آدرس سایت انتشاردهنده فایل افشا شود) همچنین توجه داشته باشید زمانی که محتوای فایل‌های پدیاف با رمز عبور حفاظت می‌شود، امکان جستجو در محتوا نیز وجود ندارد و نرم‌افزارهایی که به جستجو در محتوای این فایل‌ها روی هارددیسک شما می‌پردازند نیز قادر به جستجو درون این

فایل‌ها نخواهند بود.

در این شرایط نرم‌افزارهای متعددی برای برداشتن رمز از روی فایل پیدیاف طراحی شده، اما اگر به هیچ نرم‌افزاری دسترسی نداشته باشید نیز می‌توانید به کمک مرورگر کروم روی هر دستگاهی اعم از تلفن‌های همراه هوشمند، تبلت و رایانه این کار را انجام دهید.

روش انجام کار بسیار ساده است:

۱- مرورگر کروم را اجرا کنید.

۲- فایل پیدیاف رمزنگاری شده را با عملیات کشیدن و رها کردن به مرورگر کروم منتقل کنید. (به هر روش دیگر نیز می‌توانید فایل را در مرورگر فراخوانی کنید)

۳- رمز مورد نیاز برای مشاهده محتوای فایل را وارد کنید.

۴- به منوی File مراجعه کرده و گزینه Print را انتخاب کنید.

۵- از فهرست چاپگرهای موجود گزینه Save as PDF را انتخاب کرده و در نهایت روی save کلیک کنید.

۶- اکنون فایل جدید شما بی‌نیاز از رمز است و می‌توانید آن را به‌جای فایل اصلی روی دستگاه خود ذخیره کرده یا برای دوستانتان ارسال کنید.

منبع: jamejamonline.ir

چگونه فایل‌های با حجم بالا را ارسال کنیم؟



در طول سالها فایلها اعم از اسناد، تصاویر و نرم افزارها بزرگ و بزرگتر شده اند. تا وقتی که این فایلها روی هارد دیسک شماست، نگرانی چندانی بابت حجم آنها وجود ندارد؛ اما ماجرا وقتی بغرنج میشود که مثلا بخواهید یک فایل صد مگابایتی را برای فرد دیگری ارسال کنید.



قاعداً سراغ ایمیل مبروید که اصلی ترین راه انتقال فایلها در اینترنت است. غافل از آنکه بیشتر سرویسهای ارائه کننده ایمیل محدودیتهایی در حد چند ده مگابایت برای فایلهای ضمیمه قائل میشوند. اما ناامید نشوید! راههای مختلف دیگری برای فرستادن این فایلهای بزرگ از طریق اینترنت وجود دارد که در این مطلب به آنها خواهیم پرداخت.

از فضای ابری بهره بگیرید

یکی از بهترین راهکارها برای ارسال فایلهای با حجم بالا استفاده از سرویسهای ابری است. فضاهای ابری گوگل درایو، دراپ باکس و همچنین وان درایو مایکروسافت شاخصترین سرویسهایی است که میتوانید از آنها برای انتقال فایلهایتان کمک بگیرید.

اگر از کاربران جیمیل هستید (چه کسی نیست؟)، گوگل با اتصال میان دو سرویس گوگل درایو و جیمیل کار را بسیار راحت کرده است.

کافی است هنگام تایپ یک ایمیل جدید، از قسمت پایین به جای گزینه گیره کاغذ که فایل را به صورت عادی ضمیمه می‌کند، لوگوی گوگل‌درایو در کنار آن را کلیک کنید تا با باز شدن درایوتان در یک پنجره بتوانید فایلی را آپلود یا از فایل‌های موجود یکی را انتخاب کنید. هنگام ارسال فایل‌ها از گوگل‌درایو هم می‌توانید انتخاب کنید. این فایل به صورت ضمیمه برای گیرنده دیده شود یا به صورت لینکی به درایو. گوگل‌درایو محدودیتی برای حجم فایل آپلودی تا آن مقدار که فضای ابری‌تان اجازه دهد، ندارد.

دو سرویس دراپ‌باکس و وان‌درایو نیز برای ارسال فایل‌های بزرگ بسیار مفید است. شما می‌توانید از طریق نرم‌افزارها یا سایت این سرویس‌ها فایل‌تان را در فضای ابری آپلود کنید، سپس لینک آن را برای دیگران، چه از طریق ایمیل یا هر مسیر دیگری بفرستید. محدودیت دراپ‌باکس برای آپلود فایل‌ها از طریق وبسایتش ده گیگابایت است و وان‌درایو هم به همین اندازه محدودیت در نظر گرفته است.

استفاده از سرویس‌های انتقال آنلاین

اگر حال و حوصله ثبت‌نام یا علاقه‌ای به استفاده از سرویس‌های ابری را ندارید، سایت‌های زیادی وجود دارد که روند ارسال بی‌دردسری را بدون نیاز به ساخت اکانت در اختیارتان قرار می‌دهد. این‌گونه سایت‌ها صرفاً به عنوان یک واسطه فایل موردنظرتان را دریافت و برای مخاطب ارسال می‌کند.

سایت wetransfer.com یکی از محبوب‌ترین این سرویس‌هاست که در محیط کاربرپسند و سراسر آن می‌توانید فایل‌های مورد نظرتان را تا دو گیگابایت آپلود و به همراه یک پیام متنی ارسال کنید. این سایت دو نوع از انتقال را پیش پای شما می‌گذارد: در حالت اول فایل‌تان را آپلود و لینک دانلود آن را دریافت می‌کنید. حال این لینک را از هر راهی که خواستید می‌توانید برای مخاطبتان ارسال کنید تا با کلیک روی آن، فایل را دانلود کند.

در حالت دوم، می‌توانید آدرس ایمیل‌تان را به سایت بدهید تا خود سایت از طرف شما این فایل را برای حداکثر ۲۰ نفر بفرستد. همچنین با استفاده از نرم‌افزارهای این سرویس برای اندروید و iOS این امکان را خواهید داشت تا تصاویر و ویدئوهایی تا ده گیگابایت را مستقیم از روی گوشی‌تان انتقال دهید.

سایت‌های دیگری مانند transfer.pcloud.com، free.mailbigfile.com

یا filemail نیز وجود دارند که عملکردی شبیه wetransfer دارند، ولی با تفاوت در اندازه فایل یا عرضه ویژگی‌های خاص. برای مثال، pcloud در حالت رایگان به کاربر امکان می‌دهد فایل‌های تا پنج گیگابایت و دارای پسورد را برای حداکثر ده مخاطب ارسال کند.

همچنین سرویس filemail حجم فایل‌های قابل ارسال را به ۳۰ گیگابایت رسانده و با ارائه نرم‌افزارهای موبایل، قابلیت ارسال فایل‌های بسیار بزرگ را به صورت مستقیم از روی تلفن همراه به کاربر می‌دهد.

دقت داشته باشید در بیشتر این سرویس‌ها، فایل شما برای مدت محدودی روی سرور سایت باقی می‌ماند. برای مثال در سایت filemail.com، مدت زمان حفظ فایل هفت روز است و پس از آن مانند پیام‌های کارآگاه گجت نابود می‌شود!



تورنت هم هست

شاید فکر نمی‌کردید نام تورنت را برای این کاربرد ببینید، اما سیستم تورنت عملاً برای همین کار است؛ یعنی به اشتراک‌گذاری یک فایل حجیم میان تعداد زیادی از مخاطبان. برای این‌که درک بهتری از سیستم تورنت پیدا کنید، تصور کنید یک فایل را به تعداد زیادی بخش کوچک‌تر تقسیم کرده‌اید. مثلاً یک فایل یک گیگابایتی را می‌توان به هزار قسمت یک مگابایتی تقسیم کرد. حال اگر این قسمت‌ها به صورت تکه تکه از رایانه مبدأ به سیستم مقصد منتقل و در آنجا سر هم شود، عملاً فایل یک گیگابایتی منتقل شده است!

البته با وجود کاربردی بودن این تقسیم، مزیت اصلی تورنت در مدل

نظیر به نظیر (Peer-to-Peer) بودن آن است. به این معنا که نیازی نیست شما تمام فایل را آپلود کنید تا بعد مخاطبتان امکان دریافت آن را داشته باشد. بلکه انتقال به صورت مستقیم و مداوم از رایانه شما به رایانه مخاطب بر بستر اینترنت صورت می گیرد و تا وقتی رایانه مبدأ (یا هر سیستم دیگری در شبکه که تکه های فایل را داشته باشد) روشن و به اینترنت متصل باشد، تکه های فایل منتقل خواهد شد.

به راه انداختن یک سیستم انتقال از طریق تورنت چندان پیچیده نیست، اما کمی کار بیشتری نسبت به راه حل های بالا می طلبد. برای این کار، ابتدا یک نرم افزار تورنت مانند qBittorrent یا uTorrent را نصب می کنید و از منوی آن گزینه ساخت یک تورنت جدید را انتخاب می کنید.

برای یک تورنت جدید، فایل یا فولدری را که می خواهید به اشتراک بگذارید انتخاب کرده، سپس فهرستی از trackerها (سایت هایی که آمار اتصالات تورنت ها را نگهداری می کنند) را که می توانید به رایگان در اینترنت پیدا کنید، وارد می کنید تا فایل تورنت شما ساخته شود. حال هر کسی با داشتن این فایل تورنت و استفاده از یک نرم افزار تورنت می تواند فایل شما را دانلود کند. البته حواستان باشد که باید رایانه تان روشن و متصل به اینترنت باشد تا عمل انتقال انجام شود.

فشرده کنید!

راهکارهای اشاره شده گزینه های مناسبی برای انتقال فایل های بزرگ را در اختیارتان می گذارد، اما پیش از آن که قصد ارسال یک فایل حجیم را داشته باشید، ابتدا به فکر فشرده سازی آن باشید. نرم افزارهای فشرده سازی مانند WinRAR یا Zip-۷ با توجه به فرمت فایل و نوع داده های آن، این امکان را به شما می دهند تا حجم فایلتان را تا اندازه مطلوبی کوچک کنید.

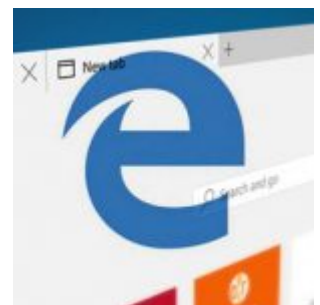
البته انتظار نداشته باشید یک فایل صد مگابایتی اندازه ۲۰ مگابایت کوچک شود، ولی از فشرده سازی پیش از ارسال فایل (بخصوص با سرعت های آپلود پایین در اینترنت کشور) هیچ گاه ضرر نخواهید کرد. بخصوص اگر فولدری با تعداد زیادی فایل کوچک دارید که می خواهید بفرستید، خواهید دید که در فشرده سازی آن کمکی شایان می کند.

فشرده سازی بجز پایین آوردن حجم فایل، مزایای دیگری هم دارد. با گذاشتن رمز عبور روی فایل هایتان می توانید مطمئن شوید فرد سومی به

محتوای آن دسترسی نخواهد یافت. همچنین نرم‌افزاری مانند WinRAR این قابلیت را به شما می‌دهد فایل‌تان را به چند بخش تقسیم کنید تا بتوانید هر بخش کوچک‌تر را به‌صورت جداگانه و با دردسر کمتر آپلود و ارسال کنید.

منبع: jamejamonline.ir

حذف خودکار تاریخچه مرورگر اِج



در ویندوز ۱۰ همچون دیگر مرورگرها، از قابلیت ذخیره‌سازی تاریخچه صفحات وب مرور شده پشتیبانی می‌کند و این قابلیت همان‌قدر که برای کاربران مفید است در مواردی نیز می‌تواند امنیت حریم خصوصی آنها را با مشکل مواجه کند.



در این شرایط اغلب کاربران برای حفظ امنیت اطلاعات خود از قابلیت مرور امن (خصوصی) کمک گرفته یا پیش از بستن مرورگر، تاریخچه ثبت شده در آن را تخلیه می‌کنند.

انجام این کار نسبتاً ساده است، اما تکرار آن به دفعات متعدد می‌تواند دشوار و خسته کننده باشد. اگر تمایل دارید با هر بار بستن مرورگر، تاریخچه ردپای ثبت شده از شما توسط مرورگر نیز به طور خودکار حذف شود کافی است این مراحل را دنبال کنید:

مرورگر اج مایکروسافت را اجرا کرده و از بالا سمت راست روی آیکون منوی اصلی که به شکل سه نقطه عمودی به نمایش درآمده کلیک کنید.

روی گزینه Settings در انتهای منوی به نمایش درآمده کلیک کنید.

پنجره را به پایین اسکرول کرده تا بخش Clear browsing data را مشاهده کنید.

در ادامه روی گزینه Choose what to clear کلیک کرده و در صفحه جدید ضمن فعال کردن موارد موردنظر برای حذف از تاریخچه مرورگر، کلید وضعیت موجود در کنار گزینه Always clear this when I close the browser را از حالت Off به On تغییر وضعیت دهید.

از حالا به بعد با هر بار بسته شدن مرورگر، تاریخچه آن نیز به طور خودکار پاک می‌شود و می‌توانید بدون نگرانی صفحات وب را در مرورگر مرور کنید.

منبع: بیتوته

برنامه های برتر کنترل دسکتاپ از راه دور



فرض کنید در کلاس درس دانشگاه نشسته‌اید و ناگهان یادتان می‌افتد،

فایل پاورپوینتی را که قرار بود امروز در کلاس ارائه کنید و روی فلش مموری ریخته بودید، با خود نیاورده‌اید. نمی‌توانید به مادرتان که در خانه است بگویید آن را برایتان ایمیل کند، چون هر بار که دستش به رایانه و صفحه کلید خورده، تنها برای گردگیری خانه بوده و از فناوری دیجیتال سر در نمی‌آورد. فاصله تا خانه هم زیاد است و گزینه رفتن به خانه را باید از ذهنتان حذف کنید. ناگهان یادتان می‌افتد قبلا از یکی از نرم‌افزارهای کنترل از راه دور دسکتاپ استفاده کرده‌اید.

بسرعت با گوشی خود به اینترنت وصل می‌شوید، نرم‌افزار مربوطه را باز و فایل مورد نظر را از راه دور روی حافظه گوشی‌تان کپی می‌کنید و همه چیز ختم به خیر می‌شود. اگر چنین تجربه‌ای را نداشته‌اید یا می‌خواهید در آینده دچار چنین کابوسی نشوید، بد نیست این مطلب را تا آخر بخوانید تا با نرم‌افزارهای کنترل دسکتاپ از راه دور بیشتر آشنا شوید.

امروزه به لطف وجود اینترنت لازم نیست حتما در برابر رایانه خود باشیم تا بتوانیم از آن استفاده کنیم. ابزارهایی موسوم به کنترل دسکتاپ از راه دور (Remote Desktop Control) این امکان را فراهم می‌کنند که در صورت لزوم از هر جایی به رایانه خود متصل شویم و حتی در صورت بروز مشکل بتوانیم آن را از راه دور حل و فصل کنیم.

نرم‌افزارهای زیادی برای کنترل دسکتاپ از راه دور وجود دارد. بسیاری از این نرم‌افزارها دارای ویژگی‌های مشترک زیادی هستند و البته هر یک، مشخصات ویژه‌ای دارند. برای انتخاب نرم‌افزار مناسب باید به نیازهای خود و نیز عوامل دیگری نظیر سیستم‌عامل مورد استفاده دقت کنیم. در ادامه به بررسی پنج نرم‌افزار محبوب کنترل دسکتاپ از راه دور می‌پردازیم.



تیم ویور

نرم افزار تیم ویور (Teameviewer) یکی از محبوب ترین نرم افزارهای کنترل دسکتاپ از راه دور است که به دلیل ویژگی های جذاب و البته رایگان بودن، طرفداران زیادی در دنیا دارد. این نرم افزار روی سیستم عامل های ویندوز، لینوکس، اندروید و آی.او.اس نصب می شود و امکان کنترل و مدیریت دسکتاپ از راه دور را به کاربر می دهد.

همچنین نیازی نیست آن را روی رایانه ای که قرار است کنترل شود نصب کنید. این نرم افزار از ویژگی هایی نظیر روشن کردن رایانه دوری که در حالت خواب (sleep) قرار دارد و برگرداندن آن به حالت خواب پس از اجرای عملیات، انتقال فایل و نیز قابلیت ارتباط از طریق گوشی هوشمند و تبلت برخوردار است.

تیم ویور امکان برقراری جلسه آنلاین بین چند کاربر را فراهم می کند. به این ترتیب در مواردی که کار با رایانه دور، پیچیده است، چند کاربر می توانند همزمان ارتباط داشته باشند و نظراتشان را با یکدیگر در میان بگذارند.

بر خلاف بسیاری از نرم افزارها که چنین قابلیت هایی را رایگان در اختیار کاربران قرار نمی دهند، تیم ویور کاملاً رایگان است و شاید این عامل، یکی از اصلی ترین دلایل جذب کاربران به آن در سراسر دنیا باشد. (هرچند در ایران خودمان اهمیت چندانی ندارد!) نصب این برنامه ساده است و می توان با استفاده از آن چند رایانه را به صورت همزمان از راه دور کنترل کرد.

اسپلش تاپ

این برنامه نیز از سیستم عامل های ویندوز، لینوکس، اندروید و

آی.او.اس پشتیبانی می‌کند و استفاده از آن برای اتصال به پنج رایانه رایگان است. یکی از برجسته‌ترین ویژگی‌های این نرم‌افزار را باید قابلیت برقراری ارتباط تصویری و صوتی بین رایانه‌ها با سرعت خوب دانست. بنابراین اگر می‌خواهید فیلمی را که روی هارد رایانه‌تان ذخیره است روی تابلت تماشا کنید و در عین حال حوصله کپی کردن یا پیدا کردن اپلیکیشن مناسب برای خواندن فرمت خاص آن فیلم را ندارید، می‌توانید براحتی از این نرم‌افزار استفاده کنید.

استفاده از این نرم‌افزار به همین جا ختم نمی‌شود و می‌توانید از همه فایل‌ها و نرم‌افزارهای موجود در یک رایانه دیگر نیز روی رایانه، گوشی یا تبلتی دیگر استفاده کنید. مشکل اصلی استفاده از این نرم‌افزار در این است که استفاده تخصصی‌تر از آن رایگان نیست.

کروم ریموت دسکتاپ

این نرم‌افزار از سیستم‌عامل‌های ویندوز و برخی نسخه‌های لینوکس پشتیبانی می‌کند و کاملاً رایگان است. کروم ریموت دسکتاپ، یکی از اپلیکیشن‌هایی است که می‌توانید روی مرورگر کروم رایانه خود نصب کنید. برای استفاده از این برنامه باید به حساب کروم خود در رایانه‌ای که قصد کنترل آن را دارید وارد شوید. با اینکه این کار سبب افزایش امنیت روند کنترل می‌شود، اما بر دشواری استفاده از آن می‌افزاید.

اصلی‌ترین مزیت این برنامه را باید امکان نصب آن روی مرورگر دانست و به همین دلیل نصب آن بسیار ساده و البته سریع است. این برنامه، ویژگی‌های افزوده چندانی ندارد و بیشتر برای رفع مشکل در رایانه مقصد یا دسترسی به فایل‌های آن به کار می‌رود.

در مقابل، پشتیبانی نکردن از تلفن‌های همراه و تبلت و نبود اپلیکیشن ویژه آن برای اندروید و آی.او.اس را باید اصلی‌ترین نقطه ضعف آن برشمرد. همچنین نباید انتظار کارهایی نظیر انتقال فایل، تماشا یا گوش دادن به فیلم‌های تصویری و صوتی به صورت استریم یا ابزارهای پشتیبانی دیگر را از این برنامه داشت. خلاصه اینکه این برنامه نصب و کاربرد ساده‌ای دارد و در عین حال عملکردهای آن بسیار محدود است.

ریموت دسکتاپ مایکروسافت و اپل

مایکروسافت و اپل هر کدام نرم‌افزار ویژه‌ای برای سیستم‌های خود دارند که با استفاده از آنها می‌توان از هر نقطه‌ای به رایانه وصل شد، به فایل‌ها دسترسی داشت و با نرم‌افزارهای مختلف کار کرد.

اگر سیستم عامل رایانه شما ویندوز است، فعال کردن نرم افزار کنترل از راه دور رایانه میکروسافت روی سرور و ارتباط با آن از طریق شبکه LAN به مراتب ساده تر از نصب یک نرم افزار دیگر برای این کار است. البته برای اتصال از طریق اینترنت به رایانه باید یک سری تنظیمات انجام دهید. همچنین نسخه ویژه تلفن همراه این نرم افزار طراحی شده است.

نرم افزار کنترل از راه دور اپل اندکی پیچیده تر از محصول میکروسافت است و در عوض امکانات بیشتری را در اختیار کاربر قرار می دهد. مدیریت کامل رایانه و انجام کارهایی نظیر به روزرسانی نرم افزارها، نصب نرم افزار و مدیریت کاربران از جمله قابلیت هایی است که این نرم افزار در اختیار کاربران خود قرار می دهد.

البته این نرم افزار با قیمت ۱۸۰ دلار به کاربران عرضه می شود، در حالی که نرم افزار میکروسافت رایگان است. با این حال نباید فراموش کرد کاربردهای نرم افزار اپل به مراتب گسترده تر از محصول میکروسافت است.

اصلی ترین ویژگی هر دو نرم افزار این است که پس از نصب اولیه روی رایانه مقصد، دیگر نیازی به انجام تنظیمات آن چنانی نیست و از آن پس بدون دردسر می توان به آن دسترسی یافت.

مودم ها هم ویروسی می شوند؟



امنیت در همه چیز مهم ترین اصل است امنیت مودم ها و دسترسی های به نت نیز از این قضیه مستثنی نیست هکر ها هم خدا خیرشان بدهد علاقه وافری به استفاده از حفره های امنیتی و اشکالات بوجود آمده تولید کنندگان است که می تواند میلیون ها کاربر را تحت اشعاع

قرار دهد

امنیت در همه چیز مهم ترین اصل است. امنیت مودم ها و دسترسی های به نت نیز از این قضیه مستثنی نیست. هکر ها هم خدا خیرشان بدهد علاقه وافری به استفاده از حفره های امنیتی و اشکالات بوجود آمده تولید کنندگان است که می تواند میلیون ها کاربر را تحت اشعاع قرار دهد. اکنون نیز کافی است با پستی دیگر از برسام همراه باشید تا از امنیت مودم یا روتر خود اطمینان کامل پیدا کنید.

تجارت مودم و ساخت آن، دست کمی از تجارت تلفن های اندروید نیست! سازندگان این وسایل ارتباطی، تعداد زیادی از دستگاه های مختلف را تولید کرده و همینطور به ارائه آپدیت های جدید نیز اهمیتی نمی دهند که کاربران را نسبت به حمله آسیب پذیر تر می کنند.

چگونه از نیمه تاریک روتر خود مطلع شویم؟

تغییر تنظیمات سرور DNS راهی است که هکر ها برای تغییر مسیر به یک دی ان اس مخرب از آن استفاده می کنند. هنگامی که به یک سایت متصل می شوید □ برای مثال سایت بانکی تان □ دی ان اس تغییر یافته شما را به یک سایت مخرب و سوء استفاده کننده به جای سایت اصلی راهنمایی می کند. البته این اتفاق معمولاً رخ نمی دهد و بعضی اوقات دی ان اس قادر به پاسخگویی نیست و شما را به سایت اصلی توسط پوشش دهنده اینترنت خودتان راهنمایی می کنند. به طور معمول درخواست های دی ان اس کند نشانه ای از داشتن چنین مشکلی است.

البته دچار شدن به چنین مشکلی بسیار واضح است و سایت های مخرب هیچ گاه از اتصالات و امنیت HTTPS استفاده نخواهند کرد.

البته هکر ها (حمله کنندگان اطلاعاتی) از تبلیغات ورودی، نتایج جستجوی تغییر یافته یا تلاش برای نصب فایل های داندلود شده نیز استفاده می کنند.

بیشترین حملات از طریق فایل های مخرب جای سازی شده جاوا اسکریپت در یک سایت می باشد. پس از این که کد جاوا اسکریپت بر یک دستگاه متصل به سیستم وای فای شما اجرا می شود، این کد توانایی دسترسی به اینترفیس را خواهد داشت که تنها در شبکه شما موجود است.

البته در این میان، بعضی از مودم ها دارای یک اینترفیس مدیریت از راه دور هستند که با یوزر و پسورد پیشفرض همراه می شود. برخی از

روبات ها می توانند این مودم ها را پیدا کرده و به آن ها دسترسی پیدا کنند. البته داستان به همین جا ختم نمی شود و می توانند تنظیمات دیگری را نیز درگیر کنند از جمله UPnP



نحوه بررسی

یکی از علائم شایع حمله به دی ان اس، مشاهده تغییر در سرور آن می باشد. در این مورد، باید به اینترفیس مبتنی بر وب مودم تان رفته و تنظیمات سرور دی ان اس را بررسی نمایید. معمولاً در این مورد در صورتی که خودتان تغییری ایجاد نکرده باشید، نحوه دی ان اس به صورت منوال یا دستی خواهد بود و شبیه به زیر می باشد.

از بین بردن و محافظت بیشتر اگر احیاناً با تغییر در دی ان اس مواجه شدید، باید به تنظیمات مودم رفته، ابتدا آن را روی حالت اتوماتیک تنظیم نمایید و سپس آن را با روش های زیر ایمن تر نمایید:

(۱) نصب آپدیت های فریم ویر؛ برای اطمینان از نصب آخرین آپدیت کافی است به سایت تولید کننده و یا پوشش دهنده اینترنت خود مراجعه نمایید.

(۲) غیر فعال سازی امکان دسترسی از راه دور؛ با رفتن به صفحه مدیریت وب مودم، این امکان را نیز غیرفعال نمایید.

(۳) گذرواژه خود را تغییر دهید؛ گذرواژه خود را به کلمه ها و

اعدادی تغییر دهید که قابل حدس نباشند.

۴) UPnP را تغییر دهید؛ حتی اگر این قابلیت آسیب پذیر هم نباشد، تکه ای از برنامه های مخرب موجود در شبکه داخلی شما می تواند از آن سوء استفاده نموده و دی اس شما را تغییر دهد زیرا هر درخواستی که از طرف شبکه لوکال شما باشد را می پذیرد.

منبع: www.aftabir.com

عادات نادرست کاربران کامپیوتر



۱- عدم نصب ابزارهای امنیتی

تصور داشتن یک زندگی مجازی آرام بدون استفاده از ابزارهای امنیتی به منظور شناسایی و حذف انواع بدافزارها عملاً دور از انتظار است. امنیت تنها در اطلاع دقیق از محتویات لینکها و باز نکردن ایمیل‌های ناشناس خلاصه نمیشود. این روزها در امان ماندن از انواع بدافزارها و تکنیک‌های پیشرفته نفوذ و دسترسی امن به اطلاعات، بدون استفاده از مجموعه‌ای حرفه‌ای از ابزارهای امنیتی عملاً غیرممکن است.

بعضی از کاربران با دلایلی غیرمنطقی مثل کند شدن سرعت کامپیوتر هنگام نصب ضدویروس و کندی سرعت اینترنت در صورت فعال بودن فایروال، باورهای اشتباه خود در زمینه عدم استفاده از ابزارهای امنیتی را توجیه کرده و حتی دیگران را هم به این کار تشویق می‌کنند.

در حالی که این دسته از کاربران باید عواقب عدم استفاده از ابزارهای امنیتی را تصور کرده و بعد تصمیم به نصب یا عدم نصب

آنها بگیرند. برای مثال شاید نصب یک ضدویروس موجب کندی نامحسوس و قابل تحمل کامپیوتر شود، اما بهتر است ساعات مدیدی که صرف نصب مجدد ویندوز و درایورها به دلیل آسیب دیدن فایل‌های سیستم‌عامل از سوی بدافزارها می‌شود را هم در نظر داشت.

ضمناً بهتر است از نصب نسخه‌های مجانی ضدویروس یا فایروال شرکت‌های غیرمعتبر بپرهیزید؛ این گونه ابزارها به جای محافظت از اطلاعات اقدام به سرقت آنها می‌کنند!

۲- عدم پشتیبان‌گیری از اطلاعات

پشیمانی برای آن دسته از کاربران تنبل که از اطلاعات خود پشتیبان تهیه نمی‌کنند، سودی نخواهد داشت. این کاربران با بهانه‌های بی‌پایه و اساس، اطلاعات را در معرض خطرهای جبران‌ناپذیر قرار می‌دهند. ضمناً از کار افتادگی‌های هارددیسک امری اجتناب‌ناپذیر است! بهتر است با شیوه‌های گوناگون پشتیبان‌گیری آشنا شده و از نرم‌افزارهای حرفه‌ای این حوزه که نیازی به دخالت شما نداشته و کار را به صورت خودکار انجام می‌دهند، استفاده نمایید. همچنین بهتر است فایل‌های پشتیبان را روی هارددیسک اکسترنال قرار دهید.

۳- عدم پشتیبان‌گیری آنلاین

یکی از بهترین و امن‌ترین روش‌های موجود برای ذخیره‌سازی کاملاً امن اطلاعات، ارسال آنها به فضای ابرهاست. سرویس Live شرکت مایکروسافت ۲۵ گیگابایت فضای کاملاً مجانی در اختیار کاربران قرار داده و امکان آپلود انواع فایل‌های حجیم را میسر کرده است. البته در Gmail گوگل هم تقریباً ۸ گیگابایت فضا در اختیار دارید. با استفاده از نرم‌افزارهایی مثل Gmail Drive یا SkyDrive Explorer می‌توان این فضاهای رایگان ابری را در قالب درایو به ویندوز اضافه کرد و با استفاده از قابلیت کشیدن و رها کردن (Drag & Drop) اقدام به پشتیبان‌گیری از داده‌های مهم نمود.

البته این راه حل فقط برای کاربران مرفه (از نوع بی‌درد) است که اینترنت پرسرعت دارند و می‌توانند به راحتی فایل‌ها را آپلود و دانلود کنند!

۴- پاسخ به هرنامه‌های تبلیغاتی

یکی از دلایل مهمی که اسپمرها را تشویق به ادامه کار می‌کند، کلیک

کاربران روی لینک‌های موجود در هرنامه‌های تبلیغاتی و حتی پاسخ به این گونه ایمیل‌هاست. بله اسپمرها کلیک روی لینک‌های Remove me یا Unsubscribe me (به منظور حذف از لیست ارسال) را پاسخی از سوی کاربران محسوب کرده، از فعال بودن آن آدرس ایمیل مطمئن شده و سیل هرنامه‌ها را با شدتی بیشتر به سوی کاربر هدایت می‌کنند.

در صورتی که پیام تبلیغاتی از سوی یک شرکت معتبر ارسال شده باشد، کلیک روی چنین گزینه‌هایی خطرناک نیست؛ البته فراموش نکنید که این روزها با حرفه‌ای‌تر شدن خرابکاران، جعل آدرس ایمیل شرکت‌های معتبر هم کار سختی نبوده و بهتر است در این گونه موارد نیز جوانب احتیاط را در نظر داشته باشید.

۵- حمل دستگاه‌های روشن

حمل نوت‌بوک روشن از اتاق خواب تا نشیمن ایرادی ندارد، اما جابه‌جایی آن مثلاً از اداره تا منزل، پیاده‌روی طولانی، هنگام بالارفتن از پله‌ها و ... بسیار خطرناک بوده و امکان وارد آمدن صدمات جدی به دستگاه وجود دارد. در چنین مواقعی که هارددیسک در حال چرخش است، امکان از کار افتادگی آن در هر لحظه وجود دارد.

از این رو توصیه می‌کنیم هنگام جابه‌جایی، نوت‌بوک یا نت‌بوک، آن را خاموش کنید، مگر اینکه مدل مورد استفاده از نمونه‌های مقاوم در برابر ضربه و تکان‌های شدید باشد. ضمناً ریسک افتادن دستگاه از دست را هم نباید فراموش کرد. در این گونه مواقع بهتر است از حالت Hibernate که در آن، محیط کار ذخیره می‌شود، استفاده نمود. دقت داشته باشید در حالت Sleep هر لحظه امکان روشن شدن اتفاقی وجود دارد.

۶- نوت‌بوک در رختخواب!

استفاده از نوت‌بوک در رختخواب اشکالی ندارد، اما پرز و کرک بالش و لحاف و ... موجب گرفتگی پورت‌ها یا بسته شدن منافذ تهویه دستگاه و در نتیجه گرم شدن و در نهایت خرابی دستگاه خواهد شد. برای رفع این مشکل بهتر است از میز نوت‌بوک به منظور حفظ جریان هوا بین نوت‌بوک و سطوح پرزدار و همچنین خنک‌سازی دستگاه توسط فن استفاده کنید. فراموش نکنید که استفاده از نوت‌بوک در حالت درازکش یا دیگر وضعیت‌های بدنی نامطلوب، اثرات سو روی سلامت شما خواهد داشت.

۷- چاپ همه چیز

در صورت وجود نسخه دیجیتال یک سند چه نیازی به چاپ نسخه کاغذی وجود دارد؟ گاهی اوقات مطالب یک وبسایت نظرتان را جلب کرده و برای مطالعه بهتر آن را در قالب Word تنظیم و چاپ می‌کنید. بهتر نیست چنین سندی را تبدیل به فایل PDF کنید و به راحتی آن را در کامپیوتر یا حتی گوشی همراه مطالعه کنید. ضمناً چاپ کمتر، برابر با قطع کمتر درختان و ایفای نقشی هر چند جزیی در نجات کره زمین است.



۸- اظهار نظرهای آنلاین

در آغاز یک روز کاری بعد از نشستن پشت میز در اداره، برگه اخراج را روبروی خود خواهید دید و متوجه از دست رفتن شغل محبوبتان خواهید شد. اگر چه باور این مسئله تا حدودی سخت است اما امکان چنین اتفاقی دور از ذهن نیست. شاید یکی از اظهارنظرهای (کامنت‌های) قدیمی‌ شما در مورد عملکرد یکی از همکاران که هم اکنون رئیس شرکت شده، علت اخراج شدن تان باشد.

البته بعید نیست در وب سایت یا وبلاگ شخصی خود، یا در نظرات

شبکه‌های اجتماعی از شرکت به خاطر بی‌کفایتی مدیران و کارکنان هم گله کرده باشید. حال یکی از مسئولان یا کارکنان بانفوذ با مشاهده چنین اظهارنظرهایی که حتی آنها را با نام مستعار منتشر کرده‌اید، موجبات بیکار شدن‌تان را فراهم کرده است؛ پس حتی نام مستعار (نام کاربری در وب سایت‌ها) خود را نزد همکاران فاش نکنید.

امروزه مسئولان با یک جستجوی ساده نام و نام خانوادگی، آدرس ایمیل یا نام مستعار، قادر به مشاهده نظرات شما در اینترنت هستند. بهتر است جوانب احتیاط را رعایت کرده و از اظهارنظرهای بی‌مورد در فضای وب خودداری نمایید.

۹- رها کردن نوت‌بوک در خودرو

سارقان زیادی منتظر سرک کشیدن به درون خودروهای پارک شده هستند تا در صورت وجود چیزی با ارزش، دست به کار شوند. اگر نوت‌بوک خود را اغلب در خودرو به همراه دارید، باید احتیاط زیادی به خرج دهید. بهتر است هنگام پیاده شدن از خودرو نوت‌بوک را نیز با خود بردارید.

ضمناً استفاده از ابزارهایی موسوم به قفل سفر یا Travel Lock هم بد نیست. قفل سفر که نمونه‌های مختلفی دارد، به نوت‌بوک متصل شده و در صورت جدا شدن صدایی ناهنجار و بسیار بلند پخش می‌کند. ضمناً در ویندوز ۷ و ویستا نیز با استفاده از ویژگی Bitlocker می‌توان کار رمزنگاری اطلاعات روی هارددیسک را به منظور عدم دسترسی دیگران به آنها انجام داد.

۱۰- عدم داشتن آدرس ایمیل اضافه

کاربران حرفه‌ای چندین آدرس ایمیل داشته و از هر کدام برای مقاصد خاص استفاده می‌کنند. برای مثال آدرس ایمیل شخصی، در اختیار دوستان درجه یک و افراد خانواده قرار گرفته و آدرس ایمیل کاری را برای مکاتبات کاری در نظر می‌گیرند.

بهتر است آدرس شخصی را در اختیار خبرنامه‌ها، سرویس‌های وب و ... قرار ندهید، چرا که پیام‌های تبلیغاتی یا اطلاع‌رسانی‌های این گونه سایت‌ها شما را کلافه خواهند کرد. برای ثبت‌نام در بعضی سایت‌ها و استفاده از امکاناتی مثل دسترسی به لینک دانلود مجبور به وارد کردن آدرس ایمیل هستید؛ چنین سایت‌ها و سرویس‌هایی ایمیل‌ها را نگهداری کرده و بعضاً تبلیغات خود را از این طریق به شما ارسال

کرده و حتی گاهی اوقات آنها را به اسپمرها می‌فروشند.

علیرغم قول عدم استفاده تجاری از ایمیل‌ها از سوی این سایت‌ها، گاهی اوقات این اتفاق نیفتاده و به بازدیدکنندگان خیانت می‌شود. فراموش نکنید حتی در صورت متعهد بودن سایت، احتمال هک شدن پایگاه داده و دسترسی هکرها به ایمیل‌ها وجود دارد. یک ایمیل اضافی ساخته و در موارد ضروری آن را در اختیار وبسایت‌ها قرار دهید.

۱۱- عدم استفاده از کلیدهای میانبر

برخی از کاربران آشنایی بسیار کمی با میانبرهای کیبورد داشته و حتی نمی‌دانند فشار دادن کلیدهای Ctrl+C کار کپی و Ctrl+V کار Paste را انجام می‌دهد. البته یادگیری تمامی میانبرهای کیبورد و عادت به استفاده از آنها کار ساده‌ای نیست، اما هر چه میانبرهای بیشتری یاد بگیرید، سرعت شما در انجام کارها بیشتر خواهد شد. از هم‌اکنون ماوس را کنار گذاشته و استفاده از میانبرهای پرکاربرد را آغاز کنید.

۱۲- نصب نرم‌افزارهای غیرضروری

“چرا ویندوزم کند شده؟” این سوالی است که به شنیدن آن عادت داریم و عوامل گوناگونی در بروز آن نقش دارند؛ احتمالاً ۳ نرم‌افزار مجزای پیام‌رسان، ۴ مرورگر اینترنتی مطرح و به همراه ۷ نوارابزار روی هر یک نصب کرده‌اید و فایل‌های زیادی روی دسکتاپ یا پوشه Documents ذخیره نموده‌اید و ...

عده‌ای عادت به تست و بررسی انواع نرم‌افزارهای غیرضروری و ناشناخته مثل انواع و اقسام پخش‌کننده‌های چندرسانه‌ای، ابزارهای امنیتی، مرورگرهای مختلف، بازی، محافظ‌های صفحه نمایش و دیگر موارد مشابه دارند. صرف‌نظر از مسایل امنیتی، نصب انواع ابزارهای غیرضروری مشکلاتی از قبیل کند شدن یا قفل کردن سیستم را برای کاربر به ارمغان می‌آورد. بهتر است چند ابزار مطرح برای نیازهای گوناگون خود در نظر گرفته و تنها از آنها استفاده نمایید.

ضمناً بسیاری از برنامه‌های ناشناخته مثل نوارابزارها به ندرت رد پایی از خود به جا گذاشته و حذف کامل آنها گاهی اوقات غیرممکن است، به طوری که تنها راهکار موجود برای حذف آنها نصب مجدد ویندوز است.

۱۳- بی توجهی به خطرات اینترنت

هر روز اخبار جدیدی در مورد جرایم اینترنتی از قبیل فاش شدن اطلاعات شخصی و قرار گرفتن عکس و فیلم‌های خانوادگی روی اینترنت در رسانه‌ها پخش می‌شود. توصیه اول برای کاهش خطرات اینترنت پرهیز از دوست‌یابی اینترنتی یا حداقل عدم اعتماد به چنین افرادی است.

هیچ‌گاه از تصاویر واقعی در پروفایل خود استفاده نکرده یا آن را به عنوان آواتار انتخاب نکنید. از قرار دادن فیلم‌ها و عکس‌های خانوادگی در اینترنت اجتناب کنید؛ اگر امکان خرابی چنین داده‌هایی وجود دارد، بهتر است آنها را روی حساب ایمیل یا فضا‌های ابری ذخیره نمایید.

ایمیل یا حساب بانکی خود را از کامپیوترهای عمومی چک نکنید، زیرا احتمال نصب Keylogger سخت‌افزاری یا نرم‌افزاری در این سیستم‌ها و در نتیجه فاش شدن اطلاعات حیاتی، بسیار بالاست.

۱۴- استفاده از رمز عبور واحد در کلیه حساب‌های کاربری

بعضی افراد برای تمام حساب‌های کاربری از جمله ایمیل، حساب بانکی، شبکه‌های اجتماعی و ... یک رمز عبور انتخاب می‌کنند. از این رو هکر با دستیابی به رمز عبور یکی از حساب‌های چنین شخصی امکان دسترسی به دیگر حساب‌ها را خواهد داشت.

از سوی دیگر انتخاب رمز عبورهای منحصر به فرد برای هر وبسایتی که در آن ثبت‌نام می‌کنید کار آسانی نیست؛ توصیه می‌کنیم از نرم‌افزارهای مدیریت رمز عبور مثل Roboform استفاده کنید.

ضمناً از قابلیت به خاطر سپاری خودکار رمز عبور در مرورگر نیز استفاده نکنید. امروزه مرورگرهای اینترنتی هدف اول خرابکاران بوده و هر لحظه احتمال نفوذ به آنها و لو رفتن رمز عبورها وجود دارد. در صورت استفاده از کامپیوتر مشترک، ریسک مشاهده رمز عبور توسط دیگران را هم باید به جان خرید.

منبع: computernews.ir

روشن کردن کامپیوتر تنها با وارد کردن اسم خود



- ۱- بعد از روشن شدن کامپیوتر دکمه DELETE را میزنیم
- ۲- از ورود به صفحه SETUP روی گزینه Power Manegment Setup میرویم
- ۳- کلید ENTER را میزنیم و به روی قسمت POWER BY KEYBOARD میرویم و دکمه ENTER را میزنیم (البته در بعضی از مواقع شاید باید ۲ بار دکمه ENTER را بزنیم)
- ۴- کلمه نام خود را مثلا ALI رو وارد میکنیم و کلید ENTER را

میزنیم و دوباره همان نام ALI را وارد میکنیم و سپس کلید ENTER را میزنیم

۵- کلید ESC را میزنیم و وارد صفحه اصلی میشویم و کلید F10 را به عنوان تایید تغییرات انجام شده میزنیم

۶- کامپیوتر RESET میشود و بعد از خاموش کردن کامپیوتر نام خود را وارد کنید تا کامپیوتر شما روشن شود

(نکته مهم: دوستان عزیز توجه کنید که کابل برق کامپیوتر هرگز از برق درنیاید چون در این صورت فقط با فشردن دکمه POWER میتوان کامپیوتر را روشن کرد)

با یادگیری ۴۰ نکته لیسانس حل مشکلات رایانه بگیرید



۱- یک کاوشگر گوگل هوشمند باشید

هنگامی که با کدهای خطای خاص یا پیغام های ایراد سیستم عامل روبرو می شوید، گوگل می تواند یک دستیار بسیار خوب و عالی در کنار شما باشد. اینکه فقط در گوگل سرچ کنید “my PC is running slowly” یا «کامپیوتر من کند شده» احتمالاً فایده چندانی ندارد. بلکه باید تا حد امکان جزئیات ایراد پیش آمده را در کنار یکدیگر ذکر کرده و آنها را با علامت + به هم ربط دهید. همچنین برای جستجو به دنبال عبارات خاصی که به دنبال آن هستید، آن را در میان علائم “” بنویسید.

۲- برنامه بازیابی سیستم یا System Restore

قابلیت بازگشت به عقب در ویندوز به شما امکان می دهد تغییرات اخیر درون رجیستری، سخت افزار و نرم افزار کامپیوتر را به حالت قبل برگردانید. و البته این کار هیچ تاثیری روی فایل های شخصی که طی این مدت در کامپیوتر اضافه کرده اید، نخواهد گذاشت. اگر در چند روز اخیر مشکلی پیش آمده، این نقطه شروع خوبی برای حل آن است. System Restore را در کنترل پنل خواهید یافت.

۳- Safe Mode

با فشردن دکمه F8 هنگام بالا آمدن کامپیوتر می توانید به منوی بوت کامپیوتر دست یابید. حال با انتخاب گزینه Safe Mode به نسخه ای از ویندوز وارد می شوید که به جز درایورهای ضروری و برخی ابزارهای اولیه، هیچ چیز دیگری در آن لود نشده و ظاهری همانند سیستم عامل مایکروسافت در دهه ۹۰ دارد! از حالت Safe Mode می توانید برای حذف برنامه ها یا ابزارها استفاده کنید. یا اینکه برنامه های عیب یابی (trubleshooting) را اجرا کنید. به خصوص این گزینه هنگامی کارایی خوبی دارد، که شما به صورت عادی نتوانید وارد ویندوز شوید.

۴- داغ شدن بیش از حد

اگر کامپیوترتان به طور تصادفی قفل می کند ولی در ظاهر هیچ مشکل نرم افزاری یا ایراد سخت افزاری خاصی ندارد، ممکن است دچار مشکل گرم کردن و داغ شدن بیش از حد باشد. بهتر است به فکر خرید فن یا خنک کننده جدیدی باشید، تا مشکل سیستم تهویه حرارتی لپ تاپ و کامپیوترتان حل شود.



۵- روشن بودن قابلیت اسکن لحظه ای

بخش زیادی از ایرادات سیستم ما (از سرعت و عملکرد پایین تا ریستارت های ناخواسته) به دلیل حضور موجودات خبیثی همچون ویروس و بدافزارها به وقوع می پیوندند. ناگفته پیداست که باید آنتی ویروس و برنامه های ضد بدافزار خود را همیشه به روز نگه دارید و علاوه بر روشن گذاردن اسکنرهای آنها، هر از گاهی به کنترل سیستم تان هم بپردازید. همچنین یک گزینه تکمیلی استفاده از دو اپلیکیشن امنیتی بسیار خوب Spybot Search & Destroy و Microsoft's own Safety Scanner در کنار نرم افزارهای امنیتی معمول سیستم است. مزیت مهم این برنامه ها آن است که با ابزارهای امنیتی قبلی سیستم تداخلی نداشته و در کنار آنها به خوبی کار خواهند کرد.

۶- پارازیت در پس زمینه

کارایی پایین و کندی که طی گذر زمان اتفاق می افتد، می تواند به دلیل برنامه ها و نرم افزارهای فراوانی باشد که روز به روز روی کامپیوتر بیشتر می شوند و اغلب آنها هم دوست دارند در پس زمینه کامپیوتر فعال بوده و مشغول انجام کاری باشند. Task Manager را

باز کنید تا میزان استفاده واقعی از رم و پردازنده کامپیوتر در حال حاضر را مشاهده کنید.

ساده ترین راه باز کردن تسک منیجر، راست کلیک روی تسک بار پایین دسک تاپ و انتخاب Task Manager است. اگر در میان سرویس ها و فرآیندهای این لیست مواردی را می یابید که با آن آشنایی ندارید یا وجود آنها در پس زمینه کامپیوتر چندان منطقی به نظر نمی رسند، برای جزئیات بیشتر یک جستجوی ساده در گوگل، بسیار راهگشا خواهد بود. پیدا کردن راهی برای حذف این برنامه ها از پس زمینه، می تواند کمک بزرگی به افزایش سرعت سیستم باشد.

۷- استارت آپ انتخابی

اگر در Task Manager مورد یا مواردی را یافتید که واقعا اضافی و به درد نخور بودند، بهتر است کنترل کنید آنها همراه با ویندوز، اجرا نشوند و بالا نیایند. برای این کار ابتدا پوشه Startup درون استارت منو را باز کرده و هر چیز به درد نخور را از درون آن حذف کنید.

برای کنترل بیشتر روی فرآیندهای استارت آپ ویندوز در ویندوز ۷، درون کادر جستجوی استارت منو عبارت msconfig را تایپ کنید. در پنجره باز شده می توانید جزئیات بیشتری در خصوص ابزارها و سرویس هایی که به طور خودکار هنگام بالا آمدن سیستم عامل همراه با آن اجرا می شوند، بیابید و آنها را کنترل کنید. برای کنترل فرآیندهای استارت آپ ویندوز ۸ هم بهتر است سری به راهنمای ساده کار با Task Manager در ویندوز ۸ بزنید. احتمالا متعجب می شوید که چه قدر سرویس های زیادی همراه ویندوز بالا می آیند.

۸- بازیابی فایل ها

هنگامی که ویندوز فایلی را پاک می کند، واقعا آن را نابود نکرده و تبدیل به کدهای ۰ و ۱ نمی کند. بلکه به سادگی تنها ارجاع به آن را از سیستم آدرس دهی خود حذف نموده و آن بخش از دیسک را به عنوان فضای خالی علامت گذاری می کند. در صورتی که هنوز آن فضا با فایل دیگری جایگزین و رونویسی نشده باشد، ممکن است شما قادر به بازیابی فایل های تان باشید. نرم افزار Recuva یکی از بهترین و قدرتمندترین ابزارهای رایگان بازیابی فایل ها در ویندوز است.

۹- ویندوز بالا نمی آید

ویندوز از چندین گزینه بازیابی سیستم خوب (از جمله Safe Mode)

بهره می برد و شما می توانید هنگام بوت نشدن سیستم از آنها استفاده کنید. هنگام بالا آمدن کامپیوتر دکمه F8 را بزنید و از منوی بوت گزینه Last Known Good Configuration را انتخاب کنید تا ویندوز سعی کند تنظیماتی را که آخرین بار به درستی طبق آنها کار می کرده ، بازیابی کرده و بالا بیاورد. راه دیگر جداسازی تمامی ابزارهای جانبی غیر ضروری از سیستم است. گاهی اوقات یک ابزار که به درستی پیکربندی نشده یا تنظیمات درستی ندارد، می تواند باعث هنگ کردن ویندوز طی فرآیند بالا آمدن شوند.

۱۰- بوق های مادر بورد

اگر پس از روشن کردن کامپیوتر مدت طولانی بدون هیچ اتفاقی می گذرد، و می بینید دستگاه با صدای بوق های بیپ مانندی خاموش شده و ویندوز بالا نمی آید، مشکل مربوط به سطوحی پایین تر از سیستم عامل و نرم افزار است. مادر بوردها معمولاً بر اساس تعداد بوق های شان به شما اخطار می دهند اشکال از چه قسمتی است. به دفترچه راهنمای کامپیوترتان مراجعه کنید تا ببینید بوق آن چه معنی دارد. اگر هم آن را نگه نداشته اید، حتماً یک نسخه آنلاین را در سایت کارخانه سازنده خواهید یافت.

۱۱- روشن نشدن دستگاه

اگر کامپیوتر یا لپ تاپ تان اصلاً روشن نمی شود، و البته مشکل از پریزهای برق هم نیست؛ بهتر است نگاهی به کابل برق دستگاه یا شارژر/ باتری آن بیاندازید. بهتر است قبل از اینکه به دنبال جایگزین کردن بخش های مهمی همچون پاور دستگاه باشید، اول با هزینه ای کم، کابل های برق و باتری های آن را کنترل و تعویض کنید.

۱۲- فروم ها

اگر به اینترنت دسترسی دارید، بهتر است قبل از اینکه سراغ گوگل بروید، سری به فروم های رسمی کارخانه سازنده یا برنامه نویسان مرتبط با محصول تان بزنید. ممکن است با راه حل ها و راهنمایی های ویژه ای برای حل مشکلی روبرو شوید که شما هم اکنون با آن روبرو هستید. استفاده از فروم های محلی مرتبط با کامپیوتر هم گاهی می تواند کارساز باشد. درباره برخی نرم افزارها، گاهی اوقات برنامه نویس ها در فروم های مرتبط با آن، به رفع باگ و ایرادهای پیش آمده می پردازد.

۱۳- از مایکروسافت بپرسید

حتما موافقید که مایکروسافت کمابیش از سیستم های تحت سیستم عامل خودش سر در آورده و می تواند به حل مشکل آنها کمک کند. بهتر است از ابزار اتوماتیک FixIt مایکروسافت کمک بگیرید. این ابزار سعی می کند به جستجوی مشکل پرداخته و پس از یافتن آن، راه حلی برای اش بیابد یا حداقل راهنمایی لازم را در اختیارتان بگذارد. برنامه Microsoft FixIt شماری از راه حل های ساده را پیش روی تان می گذارد.

۱۴- پاکسازی رجیستری

اگر چیز اشتباهی در فایل تنظیمات پر پیچ و خم رجیستری ویندوز اتفاق بیافتد، می تواند باعث بروز برخی ایرادها، قفل کردن نرم افزارها و حتی برخی ریستارت های گاه و بیگاه شود. اگر چه به هر ابزاری نمی توان اعتماد کرد، اما برنامه های فراوانی در اینترنت می توان یافت که به طور ویژه کارشان اسکن رجیستری برای یافتن و حل این مشکلات است.

Glary Registry Repair یکی از بهترین برنامه های موجود است که می تواند ایرادات رجیستری را رفع کند. به دنبال برنامه ای حرفه ای تر با امکانات بیشتر هستید؟ مسئولیت مشکلات پیش آمده با خودتان است. لطفا قبل از هر کاری، پشتیبان گیری از فایل رجیستری فراموش نشود.

۱۵- نصب دوباره ویندوز

در واقع این سیاست زمین سوخته است. اما واقعا آنقدر که فکر می کنید، موثر نیست. بسیاری از کامپیوترها و لپ تاپ ها با دیسک ریکاوری یا یک پارتیشن ریکاوری روی هاردشان عرضه می شوند. و شما با استفاده از آن می توانید دستگاه را به وضعیت اولیه اش (درست همانند هنگامی از کارخانه بیرون آمده) برگردانید. و البته لازم به ذکر نیست، پس از این کار باید تمامی نرم افزارهای تان را دوباره نصب کنید و تمامی اطلاعات شخصی روی کامپیوتر را از دست خواهید داد. پس لازم است قبل از انجام این کار، نسخه پشتیبانی از آنها تهیه کنید.

مشکلات سخت افزاری

۱۶- روی یک کامپیوتر دیگر امتحان کنید

استفاده از یک کامپیوتر دیگر برای تست موس، دوربین یا پرینتر خراب تان (یا حتی استفاده از یک پورت USB دیگر روی همین کامپیوتر) می تواند شما را از صحت عملکرد کامپیوترتان و وجود

خرابی در ابزار جانبی مطمئن کند. اگر با این آزمون ها مشکل برطرف شد، لطفاً به جای سرزنش دوربین یا موس بیچاره، به دنبال حل مشکل کامپیوترتان باشید.

۱۷- درایورهای جدید

سری به سایت کارخانه سازنده زده و جدیدترین درایورها و Firmware ها را برای ابزار مورد نظرتان دانلود کرده و آنها را نصب کنید. با این کار فایل های آسیب دیده یا مشکل دار قبلی هم جایگزین خواهند شد، آخرین پچ های حل مشکلات اضافه خواهند شد و سازگاری با سخت و نرم افزارهای جدید در ابزارهای تان بهبود خواهد یافت.

۱۸- درایورهای قدیمی

گاهی اوقات ویندوز و ابزارهای جانبی بدون سوال از شما درایورهای جدید را نصب می کنند و به ندرت، این امر موجب بروز مشکل می شود. برای حل این مشکل و بازگشت به نسخه قبلی درایور، در کنترل پنل ویندوز به Device Manager رفته و در لیست موجود روی سخت افزاری که با علامت سوال زرد مشخص شده راست کلیک کنید. گزینه Properties را انتخاب کرده و در پنجره باز شده به تب Driver بروید. اکنون می توانید با کلیک روی دکمه Roll Back Driver به درایور قدیمی برگردید.

۱۹- حذف (Uninstall) درایورها

در همان صفحه Device Manager امکان حذف کامل هرگونه ردپای درایور هر کدام از سخت افزارهای موجود در لیست را دارید. آنگاه می توانید ابزار مورد نظر را جدا کرده و با اتصال دوباره آن به کامپیوتر، پنجره فرآیند نصب درایور را از ابتدا ببینید. این گونه شاید مشکل حل شود.

از پنجره Driver Manager می توانید اقدام به آپدیت، roll back یا حذف (uninstall) درایورها کنید.

۲۰- تست حافظه (رم)

واقعاً نمی توان گفت چه زمانی حافظه یا رم دستگاه تان از کار خواهد افتاد و شما را تنها می گذارد. البته این اتفاق هم به ندرت می افتد و چندان متداول نیست. اما عدم ثبات دوره ای سیستم و قفل کردن های گاه و بیگاه اپلیکیشن ها می تواند نشانه هایی از این موضوع باشند. با کمک برنامه های عیب یابی رمی چون MemTest86+ می توانید به اسکن کامل مازول های رم نصب شده پردازید و هرگونه

مشکل در آنها را پیدا کنید.

۲۱- تست هارد درایو

هارد درایو های مدرن امروزی از سیستم درونی با نام SMART بهره می برند که سرواژه عبارت Self Monitoring And Reporting Technology یا «تکنولوژی خود-مانیتوری و گزارش دهی» است. با این تکنولوژی، دیسک ها وضعیت خود و سلامت عمومی شان را به ویندوز گزارش می کنند. ابزارهای رایگان فراوانی وجود دارند که می توانند داده های SMART را خوانده و برای تان تفسیر کنند. HDD Health یکی از این نمونه ها است که از درایو های SSD هم پشتیبانی می کند و اگر درایوهای شما نیاز به تعویض و جایگزینی داشته باشند، با نشان دادن اخطار شما را آگاه می کند.

۲۲- Windows disk checking

ویندوز هم برنامه کنترل دیسک درونی خود را دارد که به دنبال مشکلات احتمالی درون هارد دیسک های متصل به کامپیوتر می گردد. برای استفاده از آن، در ویندوز اکسپلور روی هارد درایو مورد نظر راست کلیک کرده و گزینه Properties را انتخاب کنید. آنگاه در پنجره باز شده به تب Tools بروید.

۲۳- ایراد های نمایشگر

مشکلات نمایشگر معمولا به دلیل ایراد در کارت گرافیک، خود مانیتور یا (در صورت عدم استفاده از لپ تاپ) کابل رابط رخ می دهند. در صورت امکان از یک کابل جداگانه استفاده کنید. یا اینکه سراغ گرافیک آن بورد سیستم بروید. این گونه شاید دریابید دقیقا کدام یک از حلقه های این زنجیر دچار نقص هستند. اگر مشکل از مانیتور باشد، احتمالا هیچ راهی به جز مراجعه به گارانتی، تعمیرکار یا خرید یک مانیتور جدید باقی نخواهد ماند.



۲۴- بازش کنید

حتما لازم نیست یک متخصص سخت افزار و فروشنده کامپیوتر باشید تا بتوانید نگاهی به درون کیس کامپیوترتان بیاندازید. اما قبل از هر کاری ابتدا مطمئن شوید بدن تان به زمین متصل است و الکتریسته ساکن ندارد. همچنین کامپیوتر را از برق کشیده اید.

پس از باز کردن آن به دنبال اتصالات و پیچ های قطع شده یا شل باشید. همچنین هر جا میزان زیادی گرد و خاک جمع شده، بهتر است تمیز شود. احتمالا یک قوطی هوای فشرده خیلی به کارتان بیاید. باز کردن لپ تاپ ها ممکن است بسیار مشکل تر باشد. اما در برخی مدل ها دست یابی به رم و هارد دیسک بسیار آسان است. لذا می توانید چک کنید تا اتصال آنها مشکلی نداشته باشد. احتمالا در سایت کارخانه سازنده و دفاتر راهنمای آنها کمک های بیشتری را هم می توانید بیابید.

۲۵- پشتیبان گیری

متأسفانه، زمان های بسیاری پیش می آید که شما دیگر هیچ کاری نمی توانید انجام دهید. و باید بپذیرید هارد دیسک یا کل سیستم تان به کلی نابود شده است. پس حیاتی است که نسخه های بک آپی از اطلاعات و فایل های مهم تان داشته باشید و آنها را در جای مطمئنی نگه داری کنید. احتمالا این مطلب نگهبان می تواند کمک خوبی بوده و اهمیت موضوع را دوباره گوشزد کند.

مشکلات نرم افزاری

۲۶- به روز رسانی ها

آیا برنامه ای که شما با آن درگیر هستید، آپدیت تازه ای نداده است؟ شاید برای پشتیبانی از سخت افزار جدید یا قابلیت های جدید سیستم عامل یک به روز رسانی آمده باشد؟ پس ضرری ندارد وب سایت سازنده آن را کنترل کنید. یا اینکه از ابزار آپدیت درونی که اغلب برنامه ها به آن مجهز هستند، استفاده کنید. البته در بسیاری از نرم افزارهای امروزی آپدیت ها به صورت خودکار نصب می شوند.

۲۷- نصب دوباره

اگر مشکل هنوز به قوت خود باقی است، تمام ردپاهای نرم افزار را از روی سیستم پاک کنید و سپس فرآیند نصب را از ابتدا و با نسخه تازه دانلود شده ای از برنامه یا دیسک اورجینال آن آغاز کنید. چرا؟ با این کار اطمینان می یابید هیچ فایل آسیب دیده یا خرابی روی سیستم نیست و تمام آنها را جایگزین خواهید کرد و تمامی تنظیمات نرم افزار ریست خواهند شد. برای حذف کامل تمامی ردپاهای نرم افزار می توانید از برنامه هایی همچون Revo Uninstaller استفاده کنید.

۲۸- پلاگین ها

به خاطر داشته باشید برنامه شما ممکن است به خودی خود مشکلی نداشته باشد، اما یکی از افزونه ها یا پلاگین های آن دچار ایراد باشند. سعی کنید تمامی افزونه ها و اد-اون ها را غیر فعال کرده و با فعال کردن نوبتی آنها، مشکل را پیدا کنید.

پلاگین ها و اد-اون ها ریشه بسیاری از مشکلات نرم افزاری هستند.

۲۹- پاکسازی (Clean up)

بسیاری از برنامه ها فایل های موقتی و کش تولید می کنند که گاهی می تواند باعث تداخل در روال کار عادی نرم افزار شود. پس بهتر است به دنبال راهی برای حذف این گونه فایل های جاگیر و مزاحم باشید. CCleaner یکی از برنامه های خوش دست رایگان برای انجام این کار است و می تواند فایل های موقتی یا تمپ اغلب نرم افزارها را به راحتی پاک کند.

۳۰- برنامه های ناسازگار

حتما شما هم اوقات پر دردسر و رنج آوری با برخی اپلیکیشن ها که سر ناسازگاری با برخی برنامه های دیگر سیستم داشته اند، گذرانده اید. این موضوع بیشتر در مورد ابزارهای امنیتی پیش می آید که سعی می کنند به طور همزمان کار یکسانی انجام دهند. سعی کنید به طور

موقت دیگر برنامه هایی را که ممکن است با نرم افزار مورد استفاده
تان دچار اختلال گردند، غیر فعال کنید.

مشکلات اینترنت

۳۱- نقص را پیدا کنید

قدم اول: ببینید مشکل از کجا است. ببینید آیا توسط دیگر کامپیوتر
و ابزارها می توانید به اینترنت وصل شوید. بهتر است لپ تاپ را
مستقیماً توسط کابل به روتر وصل کنید و برنامه درونی تست روتر را
اجرا کنید. شرکت خدمات دهنده اینترنت تان (ISP) هم احتمالاً در
زمینه این ایرادها ورزیده و خبره است. اگر تنها یک کامپیوتر است
که نمی تواند به اینترنت وصل شود، پس احتمالاً مشکل از تنظیمات آن
و یا کارت شبکه اش است.

۳۲- مشکلات کارت شبکه

اگر شما به آداپتور و کارت شبکه کامپیوترتان مشکوک شده اید (برای
مثال دانگل یو اس بی وایرلس)، ابتدا بخش «مشکلات سخت افزاری» را
(در بالا گفته شد) چک کنید. سعی کنید درایور آن را آپدیت کنید، آن
را حذف و دوباره نصب کنید، یا اینکه از پورت یو اس بی دیگری
استفاده کنید.

۳۳- به روز رسانی firmware

شاید به روز رسانی تازه ای برای firmware روتر و مودم مورد
استفاده تان آمده باشد، اما شرکت های خدمات اینترنت معمولاً دوست
ندارند شما کنترل زیادی روی تنظیمات داشته باشید و چیزی نگفته
اند. بهتر است به بخش پشتیبانی سایت ISP تان و همچنین کارخانه
روتر نگاهی بیاندازید. گاهی مشکلات به سادگی آپدیت یک firmware حل
می شوند.

۳۴- همه چیز را ریبت کنید

شاید این موضوع تبدیل به یک طنز شده باشد، اما بسیار اوقات
کارایی دارد. مودم یا روتر را ۳۰ تا ۶۰ ثانیه خاموش کنید و اجازه
دهید ارتباط تان با شرکت از ابتدا بازسازی شود. آنگاه دوباره آن
را روشن کنید. برای نتیجه بهتر، شاید مناسب باشد کامپیوتر تان را
هم ریستارت کرده و دوباره سعی کنید به اینترنت وصل شوید.

۳۵- کانال ها را عوض کنید

روترها معمولاً از فرکانسی همانند دیگر ابزارها (مایکروفرها،
دستگاه های کنترل کودک و...) برای ارتباط بیسیم استفاده می کنند.

این می تواند باعث کندی ارتباط شما یا اخلاص در آن شود. بهتر است دیگر ابزارها را از روتر دور کرده یا اینکه کانال مورد استفاده آن را تغییر دهید. برای انجام این کار به دفترچه راهنمای روتر و مودم تان مراجعه کنید.

استفاده از یک کانال دیگر روتر و مودم می تواند مشکل سرعت پایین اینترنت را حل کند.

۳۶- آیا سایت داون است؟

اگر با سایت خاصی مشکل دارید، بهتر است از طریق سرویسی مانند www.downforeveryoneorjustme.com آن را کنترل کنید، شاید مشکل از اینترنت و کامپیوتر شما نباشد. توجه داشته باشید اگر سرویس مهمی مانند S3 آمازون یا کلودفلر دچار مشکل شود، این می تواند به طور همزمان بر سایت های فراوانی تاثیر گذارده و آنها را از دسترس خارج کند.

۳۷- مدیریت شبکه

کمی در Network and Sharing Centre ویندوز به کاوش بپردازید تا مطمئن شوید چندین برنامه به طور همزمان سعی در مدیریت و اداره اتصال وایرلس شما ندارند. کارخانه های سازنده لپ تاپ معمولا برنامه مدیریت شبکه خودشان را روی دستگاه ها نصب می کنند. این برنامه ها تا زمانی سعی نکنند به صورت همزمان با ابزارهای درونی خود ویندوز به مدیریت شبکه بپردازند، کارشان را درست انجام می دهند.

۳۸- دردسرهای مرورگر

استفاده از یک مرورگر دیگر، بهترین راه است تا مطمئن شوید ایراد پیش آمده ربطی به مرورگر دوست داشتنی تان ندارد و از جایی دیگر آب می خورد. اگر لازم است مرورگر را سرزنش کنید، بهتر است بعد از ناسزا گفتن ها، نکات اشاره شده در بخش «مشکلات نرم افزاری» را هم نگاهی بیاندازید. به خصوص دقت کافی در کنترل بخش پلاگین و افزونه های مرورگرتان داشته باشید.

۳۹- تنظیمات فایروال

فایروال ها گاهی می توانند کج خلقی کرده و برخی سایت ها، سرویس یا برنامه ها را مسدود کنند. به تنظیمات بخش ورودی و خروجی (incoming and outgoing) فایروال تان نگاهی بیاندازید و ابزارها و سایت های بیگناه بازداشت شده را نجات دهید. اگر برای اتصال ابزار شبکه یا بازی خاصی دچار مشکل شده اید، شاید لازم باشد به

دستورالعمل فایروال جهت صدور اجازه لازم برای دسترسی برنامه ها به اینترنت، نگاهی داشته باشید. برخی ابزارهای شبکه و بازی ها به مجوزهای ویژه فایروال نیاز دارند.

۴۰- کانکشن ها را بررسی کنید.

به بخش Network and Sharing Centre ویندوز بروید و اطمینان یابید کامپیوتر شما برای اتصال به اینترنت از کانکشن صحیح استفاده می کنند. برای مثال کانکشن روشن و پیش فرض باید وایرلس، یا اتصال کابلی باشد. در حالی تمام این بخش ها باید خودشان به صورت خودکار پیکربندی و تنظیم شوند، برنامه های خرابکار یا ابزارهای امنیتی ممکن است آن را تغییر داده باشند. در این بخش همچنین یک ابزار رفع ایراد یا troubleshooter دارید که بسیار مفید و کاربردی است.