

نحوه قرار دادن رمز عبور بر روی فایل های pdf در word 2013



یکی از امکانات جدید و کاربردی موجود در Word 2013 امکان مشاهده و ویرایش فایل های PDF است که در این روش به آن به طور کامل پرداخته شده است. علاوه بر این شما می توانید از فایل های PDF تولید شده به وسیله رمز عبور نیز محافظت کنید. بدین صورت که کاربر برای مشاهده محتویات این فایل بایستی حتماً رمز عبور را وارد کند. در این ترفند به نحوه انجام این کار خواهیم پرداخت.

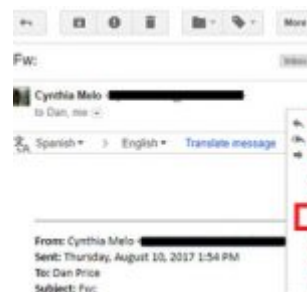


ابتدا فایل خود را در محیط Word 2013 فراخوانی کنید.
سپس از منوی File بر روی Save As کلیک کنید.
در مرحله ی بعد، محل ذخیره فایل را انتخاب نمایید.
اکنون در قسمت Save as type گزینه ی PDF را انتخاب کنید.
سپس بر روی دکمه ی Options کلیک کنید.
در پنجره ی باز شده گزینه ی Encrypt the document with a password را فعال کرده و بر روی دکمه ی OK کلیک کنید.

حال با یستی رمز عبور مورد نظر خود را وارد نموده و بر روی دکمه OK کلیک کنید.

در نهایت بر روی دکمه‌ی Save کلیک کنید تا فایل شما به صورت محافظت‌شده ذخیره شود.

بلاک تمام ایمیل‌های مزاحم در جیمیل



یکی از مشکلاتی که همواره کاربران صندوق‌های پستی از جمله جیمیل را کلافه می‌کند ایمیل‌های مزاحم است. لزوماً این ایمیل‌ها همیشه اسپم نیستند بلکه گاهی ممکن است تصمیم داشته باشید تا ایمیل‌های یکی از مخاطبان یا شرکت‌های مشهور را بلاک کنید. جیمیل برای رسیدن به این هدف راه‌کار بسیار ساده‌ای را در اختیار کاربران خود قرار داده است. با ما همراه باشید.

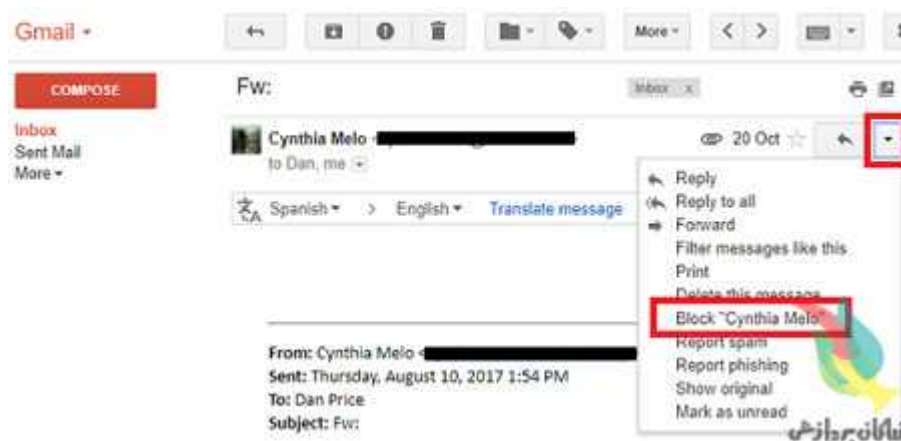
اگر از کاربران اینترنت بخواهیم که لیستی از بدترین چیزهایی که با آن برخورد می‌کنند تهیه کنند ایمیل‌های ناخواسته در کنار پیام‌های توییت و تبلیغات در صدر این فهرست جا دارند.

اما، مشکل فقط ایمیل‌های اسپم نیستند که حجم صندوق پستی را پر می‌کنند. در دنیای امروز که کاربران همیشه آنلاین هستند چقدر احتمال دارد که بتوانید برای یک مدت زمان مشخص صندوق خود را خالی نگه دارید؟

خوشبختانه، جیمیل فکر این قسمت را هم کرده و روش ساده‌ای برای بلاک کردن ایمیل‌ها از آدرس‌هایی که چندان علاقه‌ای به آن‌ها ندارید ارائه کرده است.

چگونه ایمیل‌ها را در جیمیل بلاک کنیم

- ۱- در مرورگر خود به مسیر google.com/gmail بروید و با تایپ نام کاربری و گذرواژه وارد حساب کاربری‌تان شوید.
- ۲- ایمیل فرد، شرکت یا هر آدرس رندومی که قصد بلاک کردن آنرا دارید پیدا کنید.
- ۳- ایمیل مربوطه را باز کنید.
- ۴- در همان خطی که نام و آدرس ارسال کننده وجود دارد روی فلش رو به پایین کلیک کنید.
- ۵- گزینه “[Sender’s name/address] Block” را انتخاب کنید.



چگونه ایمیل‌ها را در جیمیل آن‌بلاک کنیم

- اگر ایمیل یکی از مخاطبان خود را به‌طور تصادفی بلاک کرده‌اید، اصلاً نگران نباشید. به‌سادگی می‌توانید خودتان را از این مخمصه نجات دهید.
- ۱- جیمیل را باز کنید.
 - ۲- روی آیکن چرخ دنده در سمت راست بالای صفحه کلیک کنید.
 - ۳- وارد Settings شوید.
 - ۴- روی تب Filters and Blocked Addresses در بالای صفحه کلیک کنید.
 - ۵- به پایین صفحه بروید تا به‌گزینه The following email addresses are blocked. Messages from these addresses will appera in Spam برسید.
 - ۶- آدرسی که قصد آن‌بلاک کردن آنرا دارید هایلایت کنید.

۷- روی گزینه Unblock Selected Addresses کلیک کنید.

به همین سادگی می‌توانید ایمیل‌های مزاحم و کلافه کننده را بلاک کنید.

باج افزاری خطرناک با زبان فارسی



تایرنت «TYRANT» باج‌افزار جدیدی است که در روزهای اخیر به صورت 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 «khoodoosi 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 پیدی‌اف 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 پیدی‌اف 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

نشانه‌هایی که حکایت از هک شدن کامپیوتر شما دارد.



همیشه راحت نیست بتوانید بفهمید چه زمانی کامپیوتر شما هک شده است و خیلی سخت می‌توان این اتفاق را تشخیص داد. اما در اینجا نشانه‌هایی وجود دارد که می‌تواند دسترسی داشتن شخصی به کامپیوتر شما را افشا کند. بنابراین به موارد زیر توجه کنید و اگر هر یک از آنها برای شما نیز اتفاق افتاده است، احتمال هک شدن کامپیوتر شما بیشتر از سایر موارد است.



ناگهان سرعت عملکرد کم می‌شود

اگر اخیراً سرعت کامپیوتر شما و یا اتصال به اینترنت آن کندتر از گذشته شده است، این امکان دارد شخصی از قدرت کامپیوتر و یا پهنای باند اینترنتتان استفاده می‌کند. بسیاری از هکرها با نصب و اجرای یک اپلیکیشن در پس زمینه کامپیوتر قربانیان، منابع را در اختیار می‌گیرند و باعث کاهش سرعت همه چیز می‌شوند.

البته در اینجا به جز هک شدن کامپیوتر شما، دلایل دیگری نیز می‌تواند برای این کاهش سرعت وجود داشته باشد. کامپیوترها بعضاً به خاطر قدیمی بودن نیز با کاهش سرعت مواجه می‌شوند؛ به همین دلیل ما تنها افت ناگهانی را می‌توانیم ملاک هک شدن کامپیوتر قرار دهیم. اگر در طول روز این اتفاق برای شما افتاد، بدان معناست که چیزی مشکوک در جریان است. همین قضیه در مورد سرعت اتصال به اینترنت نیز صدق می‌کند. اگر بیش از حد معمول و بدون استفاده از آن، سرعت اینترنت شما کم شد، این بدان معناست که پهنای باندتان در حال ربهوده شدن است.



ظاهر شدن برنامه های جدید

هکرها می‌توانند بر روی کامپیوتر شما به نصب برنامه بپردازند؛ بنابراین می‌توانند به راحتی کارهای خطرناکی انجام دهند. کارهایی نظیر راه اندازی بات نت ها که می‌توانند اطلاعات بانکی و کارتهای اعتباریتان را بدزدند، کامپیوترتان را خاموش کنند و تمامی

اطلاعاتی که به دردشان میخورد را استخراج کنند. در مواقعی که شما باید شک کنید، نوار ابزار جدیدی به چشم میخورد، هشدارهای آنتی ویروس ناآشنایی دیده میشود، پاپ آپ های عجیب و غریبی نمایان میشوند و همچنین مرورگرهای جدیدی با انواع هشدارها پدیدار میشوند.

این میتواند وسوسه انگیز باشد که شما برنامه‌هایی که همیشه میخواستید را اتفاقی در کامپیوتر خود پیدا کنید؛ به خصوص اگر آنها تازه، جدید و یا گران قیمت باشند. بنابراین به خاطر داشته باشید که برنامه‌هایی را بر روی کامپیوتر خود نصب کرده‌اید و مواظب هر چیز مشکوکی که می‌بینید باشید.



غیرفعال کردن آنتی ویروس

برنامه آنتی ویروس شما باید در همه زمان فعال و در حال اجرا باشد. شما می‌توانید آیکون آن را در تسک بار کامپیوترتان نیز ببینید. اگر آن متوقف شد و یا قادر به اجرای آن نیستید، این احتمال وجود دارد که یک هکر آن را غیر فعال کرده و کنترلش می‌کند. از آنجایی که آنتی ویروس می‌تواند نشانه خوبی باشد تا شما را متوجه یک حمله کند، فکر خوبیست که شما روزانه و یا هفتگی کامپیوترتان را با آنتی ویروس اسکن کنید و البته از یک نسخه کامل آنتی ویروس قدرتمند با آپدیت‌های روزانه و هفتگی بر روی دستگاهتان استفاده کنید.

عدم توانایی در ورود

شما ممکن است هزاران بار وارد کامپیوتر خود شده باشید ولی حالا پسوردتان کار نمی‌کند. در وهله نخست، احتمال دارد شما یک کلمه را اشتباه زده باشید، پس این بار با دقت بیشتری تلاش کنید تا شاید مشکل شما حل شود. اما اگر باز هم موفق به ورود نشدید، احتمال هک شدن کامپیوتر شما زیاد است.

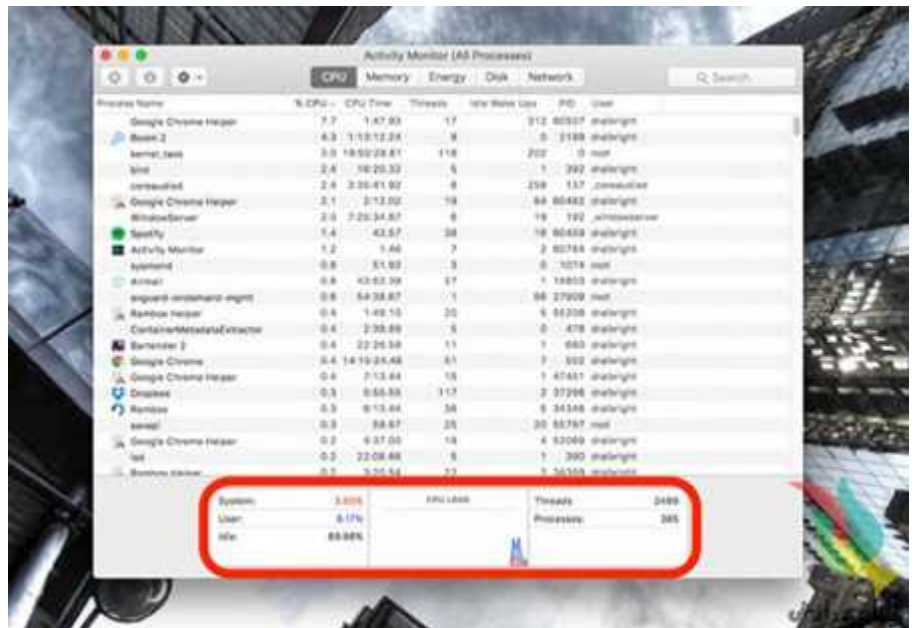
اگر درب ورود کامپیوترتان بر روی شما قفل شده، این بدان معناست که شخصی به آن نفوذ کرده و برای اینکه آزادی عمل بیشتری را در اختیار داشته باشد، جلوی دسترسی شما را گرفته است.

فعالیت‌های حجیم

زمانی که با کامپیوتر فعالیت می‌کنید، عواملی در حال فعالیت در پس زمینه سیستم عامل آن هستند که این امری طبیعیست. اما اگر شما کامپیوترتان را روشن کردید و دیدید چیزی بیشتر از حد معمول در حال فعالیت است، ممکن است چیزی مشکوک وجود داشته باشد.

اگر نشانگر ماوس شما، زمانی که آن را لمس نمی‌کنید حرکت می‌کند و یا اگر در هیستوری مرورگر شما آدرس‌هایی یافت می‌شود که هرگز به آنجا سر نزده‌اید، یا اینکه وقتی یک کار ساده همانند چک کردن ایمیل را انجام می‌دهید و هارد دیسک شما به شدت در حال انجام کار است، تمامی این‌ها می‌تواند نشانه‌هایی از هک شدن کامپیوتر شما باشد.

البته که در این بین استثنا نیز وجود دارد. به عنوان مثال ممکن است تکان خوردن ماوس به خاطر در حال اتمام بودن باتری آن باشد. یا اینکه فرزندان شما بدون اطلاع شما دست به کامپیوتر زده‌اند و از مرورگر اینترنت استفاده کرده‌اند. تسک منیجر ویندوز و یا اکتیویتی مانیتور مک را چک کنید، چرا که به شما کمک می‌کند برنامه‌های پر مصرف را شناسایی کنید.



ناتوانی در خاموش کردن

اگر شخصی کامپیوتر شما را کنترل کند، قصد دارد که همچنان کنترل را در دست داشته باشد و این بدان معناست که کامپیوتر شما نیز بایستی روشن بماند. اگر نمیتوانید طبق روال عادی و همیشگی کامپیوترتان را خاموش کنید، این امکان وجود دارد که کسی جلوی این کار را میگیرد.

همچنین طول کشیدن مدت زمان بسیار زیاد برای خاموش شدن نیز میتواند نشانهی خطرناکی باشد، چرا که هکر میخواهد کمی زمان بخرد تا بتواند کارهای خود را برای انجام در زمانی دیگر ذخیره کند.

دوستان شما فعالیت‌های زیادی را گزارش می‌دهند

آیا دوستانان اخیرا به شما گفته‌اند که ایمیل‌ها و پیام‌های متنی عجیب و غریب زیادی را برای آنها می‌فرستید؟ این میتواند یک نتیجه داشته باشد و آن هم هک شدن کامپیوتر شماست. ارسال لینک‌های مسموم، یکی از بدیهی‌ترین چیزهایی است که هکرها از این راه می‌کوشند تا اشخاص آشنا با شما را نیز هک کنند. در واقع هکرها لینک‌های خطرناکی را به ایمیل‌های شما اضافه می‌کنند.

گاهی اوقات شاید حتی ایمیل ارسالی را ببینید که هیچگاه آن را نفرستاده‌اید، اما از کامپیوتر شما فرستاده شده است. بنابراین هر کسی که به شما در این خصوص گزارش داد، فوراً همه چیز را بررسی کنید.

درخواست‌های دسترسی

بسته به تنظیمات امنیتی شما، برنامه‌ها ممکن است نیازمند درخواست مجوز دسترسی باشند. گاهی اوقات این اجازه دسترسی از طریق فایروال شما ارسال می‌شود. گاهی اوقات آن‌ها اجازه می‌خواهند تا به اجرا درآیند و یا شاید آن‌ها نیاز داشته باشند تا از اطلاعات دیگر برنامه‌ها نیز استفاده کنند. هر چیزی که اجازه دسترسی بخواهد و برای شما نا آشنا باشد، یک علامت هشدار دهنده است.

این سخت نیست که شما دست رد به سینه این درخواست‌ها بزنید، بنابراین چند ثانیه وقت صرف خواندن آن پیام کردن ارزش را دارد. مواظب برنامه‌هایی باشید که هیچگاه حتی اسم آن‌ها را نیز نشنیده‌اید.

معاملات مالی جعلی

این می‌تواند بسیار خطرناک باشد. اگر متوجه تحرکات مالی (هرچند کم) در حساب‌های بانکی خود شدید، این می‌تواند نشانه‌ای برای دزدیده شدن اطلاعات بانکی شما باشد.

اگر این نشانه‌ها را دیدیم باید چه کار کنیم؟

این موارد همگی هشدار هستند تا همه چیز را بیشتر از گذشته جدی‌تر بگیرید. این ۹ مورد می‌توانند بسیار خطرناک باشند، اما به طبع همگی دارای راه حلی هستند.

اگر کامپیوتر و یا ارتباط اینترنتی شما سنگین و کند بود، حتما باید تمامی موارد مورد نیاز را چک کنید. تسک منیجر کامپیوترتان را چک کنید و همچنین از نسخه کامل یک آنتی ویروس استفاده کنید. و در انتها تمامی داده‌های ورودی و خروجی شبکه‌های ارتباطی را نیز بررسی کنید.

منبع: beytoote

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 دانلود 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 ۰.۰.۰.۰ می باشد.

از بین بردن و محافظت بیشتر اگر احیانا 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 ان 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 ایمیل های

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 افتادگی هارد دیسک 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 هارد دیسک 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 نرم افزارهایی 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 شدن تان 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

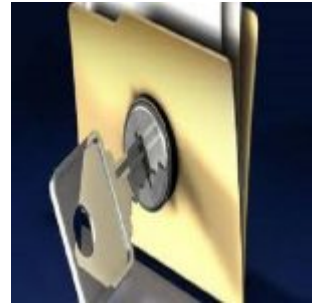
بعضی افراد برای تمام حساب‌های کاربری از جمله ایمیل، حساب بانکی، شبکه‌های اجتماعی و ... یک رمز عبور انتخاب می‌کنند. از این رو هکر با دستیابی به رمز عبور یکی از حساب‌های چنین شخصی امکان دسترسی به دیگر حساب‌ها را خواهد داشت.

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

پنهان کردن فولدر



از دو طریق می توانیم فولدری را پنهان کنیم :

۱. برای اینکه فولدری را پنهان کنید که فقط خودتان از آن خبر داشته باشید باید به روش زیر عمل کنید . اول فولدر مورد نظر خود را به حالت Rename در بیاورید سپس دکمه ی Alt را پایین نگه داشته و عدد ۰۱۶۰ را تایپ کنید و اینتر بزنید. خوب حالا فولدر شما بی نام شد. برای اینکه آیکنش را هم غیب کنید ، روی پوشه راست کلیک کنید و Properties را کلیک کنید . سپس از پنجره ی باز شده روی تب Customize کلیک کنید و بعد روی دکمه ی Change icon کلیک کنید. در میان آیکن ها یک فضای خالی هست در صورتی که این فضای خالی خودش یک آیکن است . آنرا انتخاب می کنید و پنجره ها را OK می زنید. حال فولدر شما غیب شده و دیگر کسی نمی تواند فولدر شما را باز کند.



۲ برای اینکه فولدری را پنهان کنید که فقط خودتان از آن خبر داشته باشید باید به روش زیر عمل کنید. بالای فولدر و یا فایل خود راست کلیک کرده و Properties را انتخاب کنید و بعد Hidden را تیک بزنید حالا شکل فولدر شما کمی خجل شد. برای این که کاملاً پنهان شود به Control Panel رفته و بالای Folder Options دو بار کلیک کرده و گزینه View را انتخاب کرده و گزینه Do not Show Hidden Files and Folders را تیک بزنید و ok کنید

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 مثلاً 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)