جمهوری اسلامی ایران

وزارت علوم، تحقیقات و فناوری

مدیریت حراست دانشگاه بیرجند

ویژه دانشگاهیان

بدافزارها و تهدیدات رایانه ای

شناخت و مقابله

باسمه تعالی

بدافزارها و تهدیدات رایانه ای

شناخت و مقابله

نگارش، تنظیم و طراحی جلد : سید علی خورشیدی، کارشناس حفاظت فناوری اطلاعات دانشگاه

ویراستاری : حسن زنگوئی، مدیرحراست دانشگاه

تاریخ انتشار : اردیبهشت ۱۳۹۶

سرشناسنامه : حفاظت فناوری اطلاعات .

عنوان و نام پدید آورنده : بدافزارها و تهدیدات رایانه ای(شناخت و مقابله) /سیدعلی خورشیدی .

مشخصات نشر : بیرجند، مدیریت حراست دانشگاه بیرجند، توزیع الکترونیکی، ۱۳۹۶ .

فهرست مطالب

مقدمه

مقوله بدافزار های رایانه ای و تهدیدات این حوزه بسیار مفصل است و با توجه به گسترش روز افزون، تغییر شکل و نوع آن ها لازم است بطور پیوسته مورد بازنگری قرار گیرد؛ در صورت آلوده شدن یک رایانه به بدافزار بسته به نوع آن ممکن است مشکلات مختلفی بوجود آید که در پاره ای موارد جبران آن ها هزینه های زیادی را تحمیل می کند و گاهی اوقات بازگشت به شرایط قبل ناممکن است؛ لذا بر آن شدیم تا با برگزاری دوره و تالیف کتاب آموزشی همکاران عزیز را در این مهم آگاه سازیم./

با آرزوی سلامتی و بهروزی

سیدعلی خورشیدی

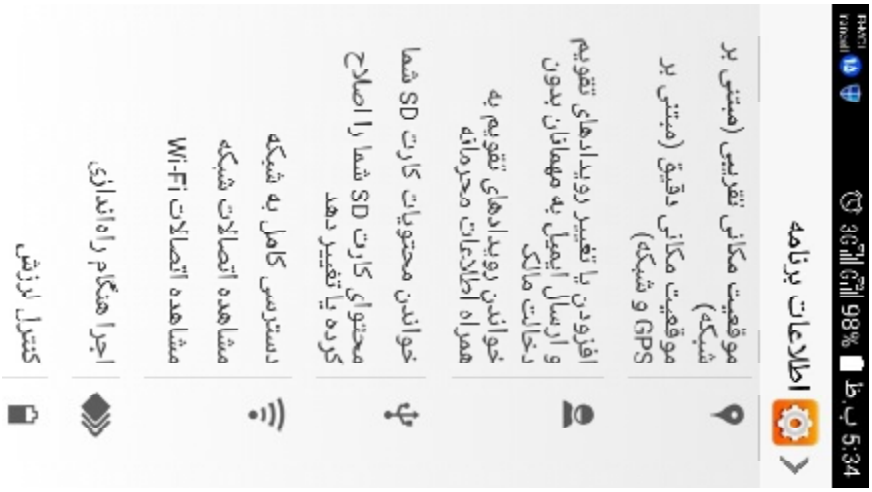
کارشناس حفاظت فناوری اطلاعات دانشگاه

اردیبهشت ۹۶

پیشگفتار

استفاده از واژه ویروس(Virus) به عنوان یک اصطلاح رایانه ای به طیفی از نرم افزارهای مخرب گفته می شود که وجه تسمیه آن به داستانی در همین زمینه برمی گردد که یک متخصص رایانه ای پول پرست برای کسب درآمد برنامه مخرب رایانه ای با نام "ویروس" می سازد که بعدها با فروش ضد آن به نام "واکسن" پولدار شود. از این داستان بعدها فیلم سینمایی هم ساخته شد. برای اولین بار در سال ۱۹۸٤ واژه ویروس در این معنا توسط "فرد کوهن" در متون آکادمیک مورد استفاده قرار گرفت.

استفاده از اصلاح بد افزار(Malware) به جای ویروس کامل تر است و طیفی چون ویروس، کرم، تروجان، باجگیر و ... را در برمی گیرد که با نیت بدخواهانه طراحی شده اند، البته بعضی نرم افزارها وجود دارند که ذاتا بد نیستند ولی روش استفاده از آن ها تهدیداتی را بوجود می آورد که به آنها ریسک افزار گفته می شود مانند بسیاری از برنامه های کاربردی گوشی های همراه که دارای دسترسی بیش از نیاز به امکانات گوشی هستند. بدافزارها هم مشابه همه برنامه های دیگر از منابع سیستم مانند حافظه و فضای دیسک سخت، توان پردازنده مرکزی و سایر منابع بهره می گیرند و می توانند اعمال خطرناکی را انجام دهند به عنوان مثال فایل های روی دیسک را پاک کرده و یا کل دیسک سخت را فرمت کنند همچنین یک ویروس می تواند مجوز دسترسی به دستگاه را از طریق شبکه و بدون احراز هویت فراهم آورد؛ در قسمت بعد لیستی از انواع بدافزارها و تهدیداتی که کاربران رایانه را مورد مواجهه قرار می دهد بیان خواهد شد.



انواع بد افزارها و تهدیدات در حوزه فناوری اطلاعات

ویروس

به برنامه مخرب کوچکی که پس از ورود به رایانه خود را تکثیر می کند ویروس گفته می شود که برای فعالیت نیاز دارد روی یک برنامه کاربردی دیگر سوار شود مثلا اگر هنگام باز کردن فایلهای ورد مشاهده می کنید که در تمامی آن ها عبارت های ناخواسته ای نوشته شده با یک ویروس سر و کار دارید که روی برنامه آفیس سوار شده است. ویروس هنگامی امکان فعال شدن را دارد که فایل آلوده باز شود، در این صورت ویروس شروع به گسترش خود در رایانه نموده و سایر فایل های موجود را نیز آلوده می نماید. انتقال این فایل ها به رایانه های دیگر و یا اشتراک فایل بین دستگاه های مختلف باعث گسترش آلودگی به این ویروس ها می شود. یک ویروس TSR که مقیم در حافظه است می تواند هر زمان و هر فایلی را که بخواهد آلوده کند.

انواع ویروس های ذیل حسب نوع خود با استقرار در محل های حیاتی، رونویسی کد فایل اجرایی، چسباندن خود به انتهای فایل میزبان و مخفی شدن به اعمال خرابکارانه خود می پردازند.

ویروس های سوار بر قطاع راه انداز Boot Sector Virus

برخی ویروس ها روی قطاع های راه انداز boot sector سوار شده منتظر فرصتی می مانند تا بتوانند خود را منتشر کرده و دستگاه های دیگری را نیز آلوده نمایند. گاهی این گونه ویروس ها به گونه ای عمل می کنند که تا زمانی که دستگاه آلوده است امکان boot کردن رایانه از روی دیسک سخت از بین برود.این ویروس ها بعد از نوشتن بر روی متن اصلی boot سعی می کنند کد اصلی را به قطاعی دیگر بر روی دیسک منتقل کرده و آن قطاع را به عنوان یک قطاع خراب (Bad Sector) علامت گذاری کنند. تمام ویروسهایی که جدول پارتیشن یا بوت سکتور را آلوده می کنند جزوTSR ها هستند.

ویروس های ماکرو Macro Virus

این نوع ویروس ها مستقیما برنامه ها را آلوده نمی کنند. هدف این دسته از ویروس ها فایل های تولید شده توسط برنامه هایی است که از زبان های برنامه نویسی ماکرویی مانند مستندات Excel یا Word استفاده می کنند. ویروس های ماکرو از طریق حافظه های قابل حمل، شبکه و یا فایل های پیوست شده به نامه های الکترونیکی قابل گسترش می باشند.

ویروس های آلوده کننده فایلFile Infecting Virus

این نوع ویروس فایل های اجرایی با پسوند exe. و com. را آلوده نموده و همزمان با اجرای این برنامه ها خود را در حافظه دستگاه بار نموده و شروع به گسترش خود و آلوده کردن سایر فایل های اجرایی سیستم می نمایند. بعضی از نمونه های این ویروس ها متن مورد نظر خود را به جای متن فایل اجرایی قرار می دهند.

ویروس های چندریختPolymorphic

این ویروس ها در هر فایل آلوده به شکلی ظاهر می شوند. با توجه به اینکه از الگوریتم های کدگذاری استفاده کرده و ردپای خود را پاک می کنند، آشکارسازی و تشخیص این گونه ویروس ها دشوار است.

ویروس های مخفیHidden

این ویروس ها سعی می کنند خود را از سیستم عامل و نرم افزارهای ضدویروس مخفی نگه دارند. برای این کار ویروس در حافظه مقیم شده و حائل دسترسی به سیستم عامل می شود به این ترتیب نرم افزارهای ضدویروس هم فریب خورده و این تصور به وجود می آید که هیچ ویروسی در رایانه وجود ندارد. این ویروس ها کاربر را هم فریب داده و استفاده از حافظه را به صورت مخفیانه انجام می دهند.

ویروس های ترکیبی

رایج ترین انواع این ویروس ها ترکیبی از ویروس های boot sector و file infecting می باشد. ترکیب انواع دیگر ویروس ها هم امکان پذیر است.

کرم Worm

بد افزاری است که برای فعالیت به میزبان نیاز ندارد و مستقل عمل می نماید، همچنین با تکثیر خود روی شبکه می تواند رایانه ها را دچار اخلال کند مثلا اگر روی میز کار شما پیغام های ناخواسته ای مشاهده می شود با یک کرم روبرو شده اید. کرم ها برنامه هایی هستند که مشابه ویروس ها توان تکثیر کردن خود را دارند، ولی برعکس آنها برای گسترش خود نیاز به برنامه های دیگری ندارند تا آنها را آلوده کرده و تحت عنوان فایل های آلوده اقدام به انتقال و آلوده کردن دستگاه های دیگر نمایند. کرم ها معمولا از نقاط آسیب پذیر برنامه های شبکه برای توزیع سریع و وسیع خود استفاده می نمایند.

اسب تراوا یا تروجان

اشاره به داستانی دارد که در آن یونانیان از یک اسب چوبی بزرگ برای فریب دشمن استفاده کردند. این گونه بد افزارها ظاهر مفید ولی باطن مخرب دارند مثلا شما یک بازی کوچک و جذاب از اینترنت دانلود کرده تا استفاده کنید ولی در حقیقت این برنامه اطلاعات مهم شما را به سرقت می برد. اسب های تروا تظاهر می کنند که کاری خاص را انجام می دهند ولی در عمل برای هدف دیگری ساخته شده اند، همان برنامه ای که وانمود می کند که یک بازی است در واقع اجازه دسترسی از راه دور یک کاربر به رایانه شما را فراهم می آورد. عملکرد اسب تروا ممکن است هر گونه فعالیت نامطلوب برای کاربر باشد؛ مانند تخریب اطلاعات کاربر یا ایجاد روشی برای عبور از سد نظارتهای معمول برای دسترس غیر مجاز به رایانه آلوده. اغلب برنامه های هک آلوده به تروجان هایی است که هکرها برای نفوذ به سامانه های دیگر و استفاده از آن سامانه برای حمله به سایر سامانه ها طراحی کرده اند.

ابزار جاسوسی Spyware

برنامه است که مخفیانه روی رایانه قربانی نصب می شود(احتمالا در قالب یک اسب تراوا)و از اطلاعات مختلفی که جمع آوری کرده برای مقاصد خاصی استفاده کرده و امنیت او را تهدید می کند.مرورگرها یکی از بستر های مهم توسعه و گسترش آن ها هستند.

ضبط کننده ضربات صفحه کلید یا Key Logger

ابزاری است که دنباله کلیدهایی که کاربر بر روی صفحه کلید رایانه می فشارد، را ثبت می کند و این امکان را دارند که گزارش حروف تایپ شده را به رایانه ای دیگر بر روی شبکه ارسال کنند. امکان ارسال اطلاعات ذخیره شده از طریق Email هم وجود دارد. این ابزار که به صورت های سخت افزاری و نرم افزاری تولید شده و در دسترس است در موارد متنوع و با کاربردهای مختلف به کار می رود. نمونه های مختلف Key logger مقدار کمی از منابع سیستم شامل حافظه و پردازنده را مورد استفاده قرار می دهند. علاوه بر این در Task manager و لیست فرایندهای سیستم هم ظاهر نمی شوند و همچنین فایلی که نرم افزار برای ثبت اطلاعات از آن بهره می گیرد نیز مخفی است، بنابراین تشخیص آن ها بر روی دستگاه به سادگی امکان پذیر نیست. علی رغم اهمیت زیادی که این ابزارها در از بین رفتن حریم شخصی

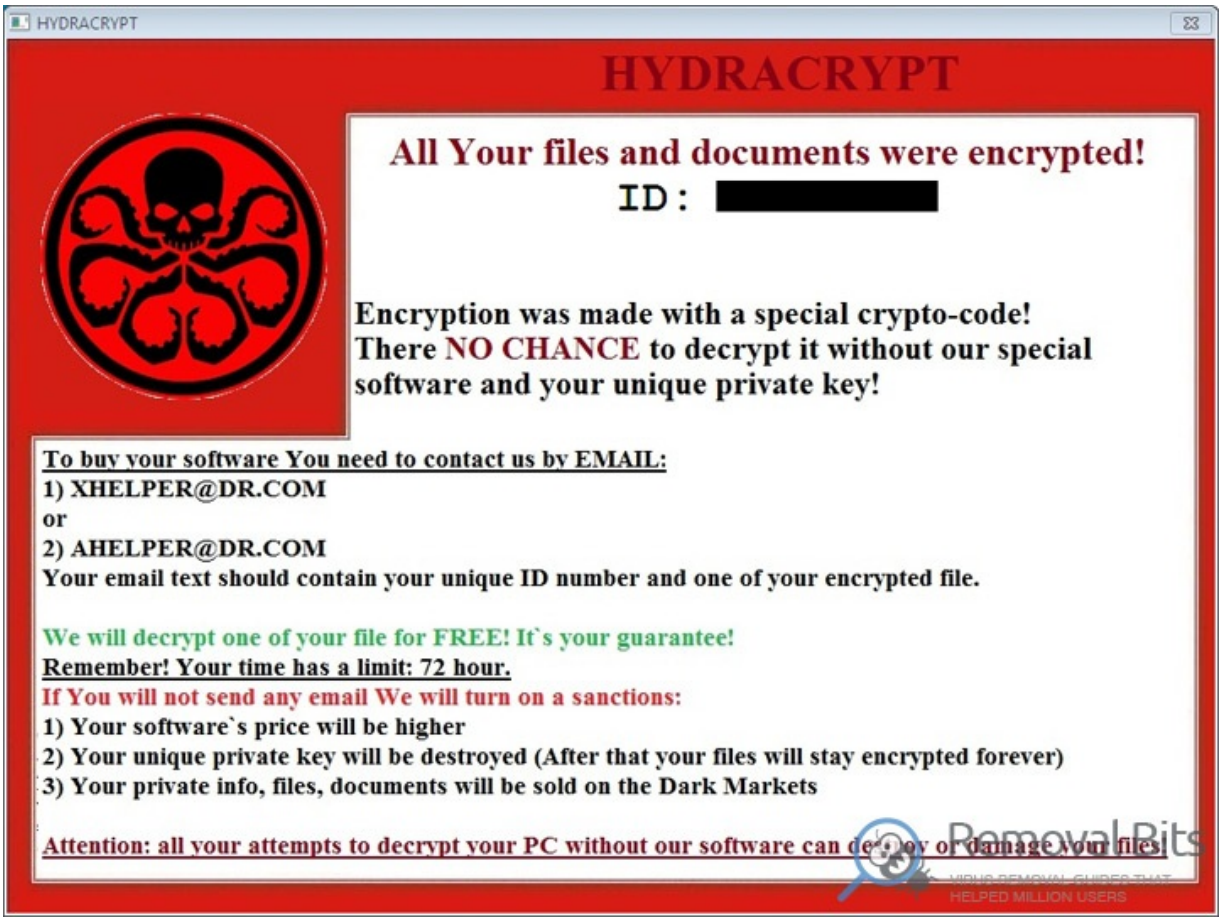
افراد و سرقت اطلاعات آن ها دارند، توجه زیادی به آن ها نمی شود شاید دلیل این امر شهرت بیشتر ویروس ها، اسب های تروا، کرم ها و شناخت بیشتر نسبت به آن ها است. بعضی از Key logger ها اطلاعات خاصی را ثبت و گزارش می کنند. لیست URL هایی که توسط کاربر دستگاه مشاهده شده و یا پیام هایی که در جریان Chat بین کاربر و دیگران رد و بدل می شود، جزء این گروه از اطلاعات می باشند .قابلیتی که تعدادی از Key logger ها دارند گرفتن عکس از صفحه رایانه در فواصل زمانی قابل تنظیم است. به این ترتیب مشخص می شود که چه برنامه هایی بر روی رایانه نصب و در حال اجرا می باشند، چه فایل هایی بر روی Desktop دستگاه قرار دارد و چه فعالیت هایی بر روی دستگاه انجام می شود. برخی از والدین که همواره نگران نحوه استفاده فرزندان خود از اینترنت هستند، با توجه به وجود انواع سایت ها و مراکز اطلاع رسانی، می خواهند کنترل بیشتری بر استفاده از اینترنت فرزندان خود داشته باشند، حداقل خواسته آن ها این است که بدانند فرزندانشان چه سایت هایی را مشاهده می نمایند و یا با چه کسانی چت می کنند. در چنین مواردی استفاده از این ابزار می تواند کمکی باشد برای والدینی که نگران سلامت روانی فرزندان خود بوده و نسبت به تربیت آنها دغدغه های خاص خود را دارند.

بمب زمانی یا منطقی

کد مخربی است که تا شرایط خاصی فراهم نشود اجرا نمی شود مثلا گاهی اوقات گروه های هکری تهدید می کنند که در زمان خاصی در یک شبکه یا وبگاه اختلال ایجاد خواهند کرد بنابراین در زمان مذکور بدافزار نصب شده روی سیستم قربانیان فعال خواهد شد.

باجگیر Ransom ware

منجمله بدترین بدافزارهای رایانه ای است که پس از اجرا با رمز کردن فایل های رایانه ای برای باز کردن آنها از کاربر درخواست واریز پول می کند و تقریبا هیچ راهکار موثری برای باز گرداندن فایل های رمز شده بجز استفاده از فایل های پشتیبان وجود ندارد. پیش بینی می شود در آینده این بدافزار قربانیان بسیاری را در کشور مخصوصا در حوزه تلفن همراه داشته باشد.



کدهای انکار سرویس DOS

با ایجاد درخواست های بسیار زیاد روی منابع رایانه قربانی آن را از کار می اندازند مثلا حلقه کدی وجود دارد که با تکرار مکرر خود و بازکردن صفحات بسیار زیاد باعث مزاحمت برای کاربر می شود. نوعی از این کدها باید همزمان روی چند رایانه انجام شود که به آن انکار سرویس توزیع شده گفته می شود.

کدهای سوء استفاده

این بدافزارها از آسیب پذیری های امنیتی شناخته شده یا کشف نشده موجود در نرم افزارهای کاربردی استفاده می کنند.

ابزارهای دسترسی ریشه Root Kit

مجموعه ابزارهای کوچکی است که یک حساب کاربری جدید با بالاترین سطوح دسترسی روی رایانه قربانی ایجاد می کند تا مهاجم حداکثر استفاده را از آن ببرد.

اسکریپ های مخرب

یک فایل است که حاوی دستورات مهاجم می باشد و اغلب در محیط مرورگرها و نرم افزارهای کاربردی اجرا می شود.

هرزنامه ها Spam

ایمیل های ناخواسته ای هستند که اغلب با اهداف تجاری تولید می شوند و با آزار دادن کاربران سلامت فضای تبادل ایمیل را مورد تهدید قرار می دهند.

نرم افزارهای گول زدن و حملات فریب

برخی نرم افزارها صرفا برای گول زدن کاربر طراحی شده اند تا کاری را انجام دهد ولی خودشان حاوی کد مخرب نیستند مانند پیامک و ایمیلی که به شما رسیده و شما را به طریقی گول می زند تا آن را برای دیگران ارسال کنید که جز صرف وقت و منابع چیزی در پی ندارد؛ همچنین وب سایت ها و ایمیل های جعلی و با ظاهر کاملا متقاعد کننده خود در کمین کاربران اینترنتی هستند.

هراس افزارها

هراس افزار یک نرم افزار به ظاهر معتبر است و سعی می کند کاربر را قانع کند که رایانه او آلوده شده است مثلا پنجره آنتی ویروس را شبیه سازی کرده و اسکنی دروغین انجام داده و رایانه شما را بسیار آلوده جلوه می دهد و به این بهانه نرم افزار تقلبی خود را عرضه می کند.

دیالرها و نرم افزارهای تماس گیرنده

در گذشته که از اینترنت خط تلفنی با کارت اینترنت(Dial up) بیشتر استفاده می شد گزارش هایی در مورد افزایش هزینه تلفن داده می شد که مشخصا به علت استفاده از تماس گیرنده ها بود که به نحوی روی رایانه قربانی نصب شده و با برقراری تماس با یک کشور خارجی ترافیک اینترنت را از روی آن عبور داده و بعضی از آن به عنوان فیلتر شکن استفاده می کردند.

پروکسی ها و فیلترشکن ها

هنگاهی که از آن ها استفاده می شـود ترافیـک اینترنتـی بـرای متولیـان آن هـا قابـل مشـاهده بوده و خطرات بیشمار دیگری هم دارد که به آن ها اشاره خواهیم کرد.

کوکی ها و ابزارهای تبلیغاتی

کوکی یک فایل متنی است که از طرف سرویس دهنده روی رایانه کاربر ذخیره شده و در مراجعات بعدی به آن سرویس دهنده برای شناسایی وی به کار می رود و مانند ابزار تبلیغاتی که طبق توافق کاربر روی رایانه او نصب می شود می توانند باعث ایجاد مزاحمت شده و حریم شخصی کاربر را تهدید نمایند.

روش های ورود بدافزارها به رایانه

مهندسی اجتماعی

تقریبا تمام بدافزارها برای ورود به رایانه و اجرا از ترفندهای مهندسی اجتماعی استفاده می کنند. مهندسی اجتماعی عبارت است از به کار بردن روش هایی که شما را متقاعد می کند کاری را که دیگران می خواهند انجام دهید در نتیجه روش های ورود و اجرای بد افزارها با که از قرار زیر است با چاشنی مهندسی اجتماعی همراه است.

وب گردی

توسعه دهندگان بدافزارها شناخت جامعی از کاربران، فرهنگ و محیط آن ها دارند و بطور مثال می دانند که ایرانی ها بخشی از اوقات فراغت خود را به وبگردی می پردازند و می دانند که بیشتر دنبال چه عناوینی هستید بنابراین از لینک های جذاب و فریبنده استفاده می کنند؛ در ماجرای فوت مرحوم پاشایی درخواست دانلود آلبوم های وی افزایش یافت بطوری که از طریق استفاده از لینک های آلوده چندین رایانه محیط ما آلوده شدند؛ جالب است بدانید که اولین نوع باج افزار ها در ایالات متحده در قالب آرم پلیس فدرال افرادی را که اقدام به مشاهده سایت های جنسی کودکان کرده بودند با ترساندن از این جرم و بدون رمز کردن فایل ها وادار به پرداخت باج می کردند.

دانلود از اینترنت

بسیاری از اوقات که نمی دانید در اینترنت واقعا دنبال چه هستید به راحتی در دام تله های مهندسی اجتماعی می افتید. دانلود کردن یک نرم افزار از یک وبلاگ به مراتب خطرناک تر از دانلود آن از یک وبسایت است. برخی از نرم افزارهای دانلود کردن نیز در قالب تروجان اقدام به جاسوسی از فعایت های شما می نمایند.

حافظه های قابل حمل آلوده

معمولا عادت کرده ایم که پس از اتصال حافظه سریعا روی منو باز شده بدون توجه به عملکرد آن کلیک کرده یا قبل از بررسی آن توسط آنتی ویروس آنرا باز کنیم.

استفاده از نرم افزارهای قفل شکسته

اگرچه تقریبا بیشتر نرم افزارهایی که ما استفاده می کنیم همینطور است ولی اینرا بدانید که در این حالت امکان تزریق کدهای مخرب در داخل این نرم افزارها بسیار زیاد است.

عدم توجه کافی به پیوست های ایمیل

یکی از راه های انتقال اصلی بدافزارها باز کردن ایمیل های ناشناس و مشاهده پیوست آن ها است.

تایید کردن پیغام های صادره توسط سیستم عامل یا نرم افزارها بدون خواندن متن آن ها

از بین بردن این عادت بد که تقریبا بین تمام کاربران ایرانی شایع است کاربسیار سختی است. مباحثی در این مورد مطرح نموده و توجه شما را به آن جلب می نماییم:

توجه به عنوان کادر محاوره ای

توجه به آیکن و شکل کادر محاوره ای

توجه به دکمه های کادر محاوره ای

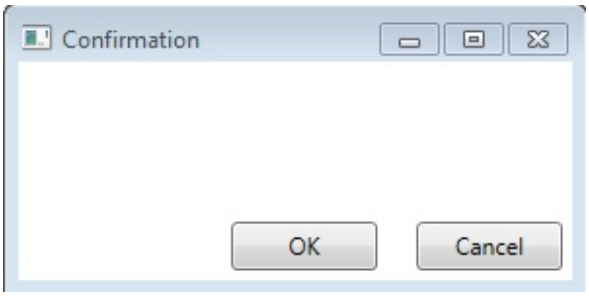
با دقت به عنوان و آیکن (تعجب) باید به قدر کافی در مورد اجرا یا عدم اجرای آن ملاحظه کنیم. بستن کادرهای مشکوک همواره توصیه می شود.

تک دکمه ok

معمولا حالت اطلاع رسانی دارد و در مورد عملی که انجام گرفته خبر می دهد. با مطالعه متن آن می توانید ضمن مطلع شدن از آن اگر عمل مطلوبی نیست سعی در رفع آن کنید. این کادرها ممکن است دکمه close را در نوار عنوان نداشته باشند.

دکمه های ok/cancel

می خواهد تایید انجام کاری را از شما بگیرد، آن را کاملا مطالعه کنید. معمولا این کادرها تعبیه شده پیش فرض برنامه نویسی هستند و تقریبا امکان ندارد کاری برخلاف مسمی خود(بله/لغو)انجام دهند؛ اما این امکان وجود دارد که متن کادر حالت منفی داشته باشد و بله/لغو معنای کلی متفاوتی پیدا کند. این پنجره ها در صورتی که دکمه close را در نوار عنوان نداشته باشند خطرناکتر هستند.



دکمه های yes/no

خطر ناک ترین نوع کادرهای محاوره ای هستند. اینکه عملکردی خلاف معنی خود انجام دهند به مرام و وجدان نویسنده آن بستگی دارد که البته معمولا با مرام هستند! ولی اینکه کادر متنی با محتوی منفی داشته باشند محتمل است. در صورت عدم اطمینان اینگونه کادرها بهتر است بسته شوند.

عدم استفاده از آنتی ویروس یا دیواره آتش یا عدم بروز رسانی و تنظیم ناکارآمد آن ها

استفاده غیر ضروری از حساب کاربری نوع مدیر

روی سیستم عامل ها انواع کاربری متفاوتی با امکانات و سطوح دسترسی متفاوتی وجود دارد مثلا کاربر نوع استاندارد در سیستم عامل ویندوز ۷ برخلاف کاربرمدیر اجازه نصب نرم افزارهای مخرب یا مفید را ندارد.

استفاده نامطمئن از افزونه ها و درشت دستورات مرورگرها

عدم نصب و بروز رسانی اصلاحیه های امنیتی سیستم عامل و نرم افزارهای کاربردی

گفته شد که برخی از بدافزارها از آسیب پذیری های موجود در نرم افزارها و سیستم عامل سوء استفاده می کنند بنابراین هرچند مدتی توسعه دهندگان آن ها برای مقابله، اصلاحیه هایی را منتشر می نمایند که عدم استفاده از آن ها مجرای سوء استفاده را همچنان باز خواهد گذاشت.

هدف از ایجاد و توسعه بدافزار

نکته ای که در اینجا باید به آن توجه نمود این است که میان نوشتن یک بدافزار و استفاده ترکیبی از کدها و اسکریپت مخربی که قبلا تولید شده است تفاوت بسیاری وجود دارد بنابراین به نوجوانان عاشق رایانه و خرابکاری که اسکریپ های مخرب را به دست آورده و روی رایانه دیگران اجرا می کنند نوجوانان اسکریپتی گفته می شود که اغلب با چنین افرادی سر و کار داریم، افراد یا گروه هایی هم هستند که با اهداف شخصی و مجرمانه یا باهدف های مالی به رایانه ها و سامانه ها نفوذ کرده و مشکل ساز می شوند که به آنها هکر کلاه سیاه گفته می شود، در مقابل آن ها هکرهای کلاه سفید قرار دارند که با اقدامات ضد امنیتی خود موجب پیدا شدن آسیب پذیری ها و افزایش امنیت سامانه ها می شوند و اغلب نوجوانان اسکریپتی هدایت شده هستند.

در این میان دولت ها هم بصورت سامان یافته برای خرابکاری، جاسوسی و ضربه زدن به حریف اقدام به تولید و انتشار بدافزارها در سایر کشورها می نمایند؛ در کل می توان گفت یک نویسنده بدافزار یا یک هکر که از یک بدافزار یا آسیب پذیری استفاده کرده تا به یک سیستم نفوذ کند صرف نظر اینکه شخص، گروه یا یک دولت باشد و چه انگیزه هایی مانند رفع عقده حقارت و اثبات خود، انتقام گیری و دشمنی و کسب درآمد مالی داشته باشد برای اهداف زیر حمله می کند:

۱- تخریب

۲- تحریف

۳- سرقت

٤- شنود

٥- اختلال در ارایه سرویس

پیشگیری و کنترل

مقابله با بد افزارها را مانند مقابله با ویروس های بیولوژیکی در دو مرحله پیش گیری و درمان مورد بحث قرار می دهیم و قطعا مرحله پیشگیری بسیار مهمتر می باشد.

الف) نصب و بروز رسانی های آنتی ویروس ها و بکارگیری دیواره های آتش

نرم‌افزار ضدویروس (Anti Virus) که با نام‌های ویروس‌یاب و ویروس‌کش هم شناخته می‌شود، نرم‌افزاری است که با مشاهده و بررسی محتوای پرونده‌ها به دنبال الگوهای آشنای ویروس ها یا کرم‌های اینترنتی می‌گردد. در صورت مشاهده این الگوها که به آن امضای ویروس (Virus Signature) گفته می‌شود، از ورود آن به رایانه شما و اجرا شدن‌اش جلوگیری می‌کند و یا به شما هشدار لازم را می‌دهد و از شما دستور می‌گیرد که آیا فایل را حذف کند و یا سعی نماید آن را اصلاح و پاکسازی کند. شرکتهای سازنده نرم‌افزارهای ضدویروس، با ساخته شدن ویروسهای جدید، الگوهای نرم افزاری آن ها را کشف و جمع آوری می‌کنند و به همین علت اغلب لازم است تا این نرم‌افزارها مدام به‌روزرسانی (Update)شوند تا الگوهای جدید ویروسها را دریافت کنند.

امروزه استفاده از آنتی ویروس روی هر رایانه ای ضروری است و در صورتی که روی رایانه شما اطلاعات مهمی ذخیره شده است هزینه ای که برای تهیه و بروز رسانی آنتی ویروس خود پرداخت می نمایید قطعا در برابر ارزش اطلاعات شما ناچیز است اما اگر از آنتی ویروس های قفل شکسته و آپدیت آفلاین استفاده می کنید بسیار بیشتر در معرض خطر هستید. با توجه به گسترش بد افزارها و تغییر شکل آن ها، پایگاه داده آنتی ویروس باید مرتب بروز رسانی شود تا کارایی لازم را داشته باشد.

ویژگی‌های یک نرم‌افزار ضد ویروس مناسب

همانطور که برای هر محصولی (چه نرم‌افزاری و چه سخت‌افزاری) آزمون‌هایی وجود دارد که کیفیت و شایستگی آن را تعیین می‌کند، چنین سنجش‌هایی برای یک نرم‌افزار ضد ویروس هم وجود دارد. یکی از آزمون‌ها با نام آزمون DURCH شناخته می‌شود که نام آن سرواژه‌ای است که از حروف ابتدایی بخش‌های پنجگانه این آزمون تشکیل شده‌اند. بنابر آزمون DURCH یک نرم‌افزار ضدویروس مناسب باید بتواند به نیازهای زیر پاسخ دهد:

۱) آزمون درخواست **:(Demand)** باید بتواند هنگامی که می‌خواهید به یک پرونده یا صفحه اینترنتی یا یک رایانامه دسترسی یابید، آن را بررسی کند.
۲) آزمون به‌روزرسانی **:(Update)** به این معنی که نرم‌افزار باید بتواند در بازه‌های زمانی مشخص بانک اطلاعاتی خود که شامل امضای ویروس‌ها است را بروز کند.
۳) آزمون واکنش **:(Respond)** اینکه نرم افزار بتواند تمامی رفتارهای منطقی در برخورد با یک ویروس را از خود نشان دهد. پرونده آلوده را دوباره‌سازی و تمیز کند و یا آن را حذف نماید.
٤) آزمون وارسی **:(Check)** باید بتواند تمام فایلها از نوع مختلف که می‌توانند محلی برای پنهان شدن ویروس باشند را کنترل کند.
۵) آزمون اکتشاف **:(Heuristics)** به این معنی که نرم افزار باید با وجود نداشتن الگوی همه ویروس ها، بتواند خطر و احتمال وجود ویروس را تشخیص دهد. این رفتار نیازمند هوشمندی نسبی نرم‌افزار و استفاه آن از روشهای اکتشافی است.

نحوه عمل آنتی ویروس ها معمولا به دو صورت مبتنی بر امضا یا مبتنی بر رفتار می باشد و همین قدر که بدانید در روش مبتنی بر امضا آنتی ویروس دارای یک لغت نامه شامل الگوهایی از ویروس های شناسایی شده است و در رایانه شما به دنبال آن ها می گردد ولی در روش مبتی بر رفتار، رفتار مشکوک یک برنامه

مثلا درخواست دسترسی بی مورد به فایل های سیستمی باعث شناسایی بد افزار می گردد. برخی از آنتی ویروس ها از ترکیب این دو روش استفاده کرده و علاوه بر کنترل هوشمند رخدادهای رایانه ای فایل ها را در زمان اجرا، باز و بسته شدن، ایمیل یا دانلود شدن بررسی می نمایند.

اقدامات آنتی ویروس ها در برابر بدافزارهای کشف شده

Clean : پاک کردن آلودگی از فایل و تحویل فایل سالم مانند رفع ویروس از بدن بیمار با تزریق دارو.

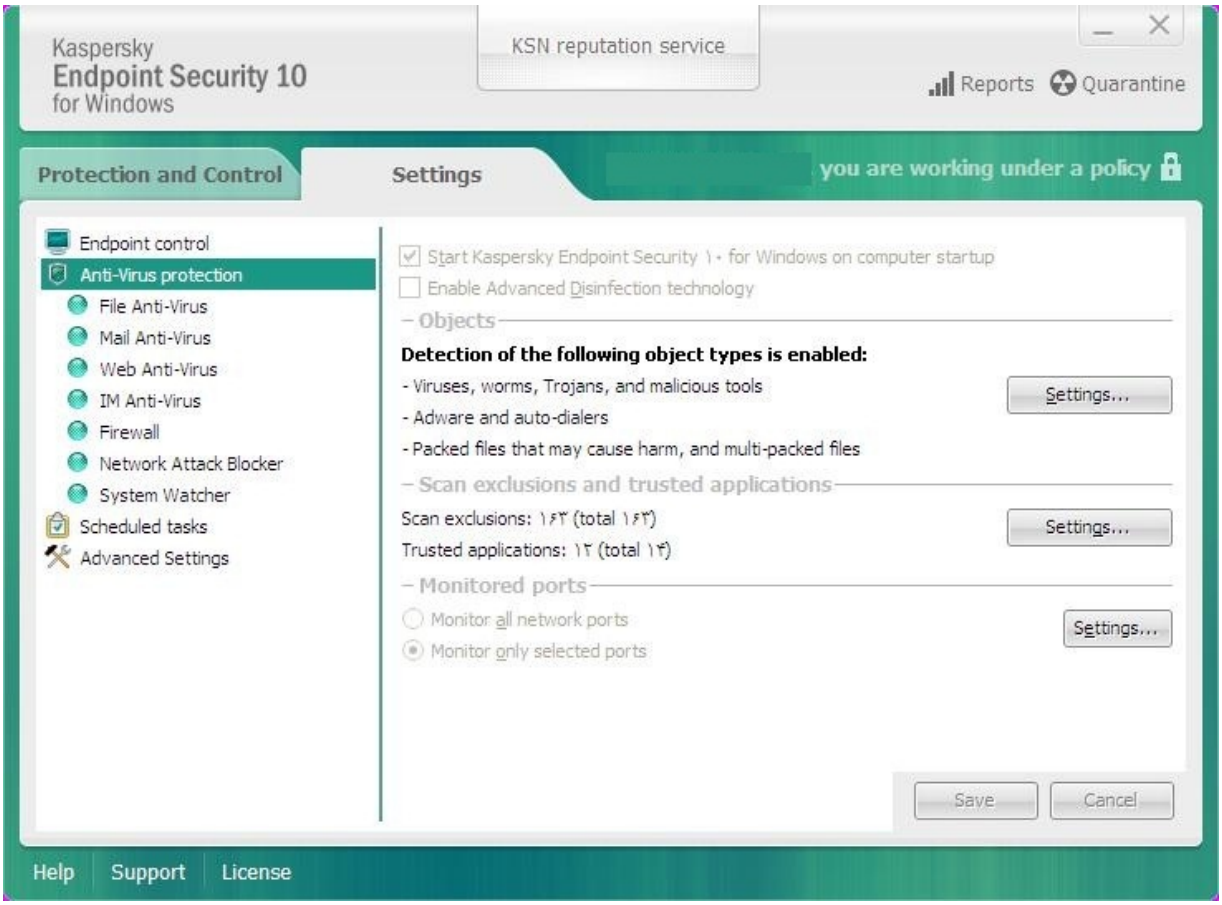
Delete : از بین بردن آلودگی به همراه فایل آلوده در صورتی که فایل آلوده خود بد افزار بوده یا امکان از بین بردن صرف آلودگی امکان پذیر نباشد مانند اینکه در زمان های گذشته انسان های دچار بیماری های لاعلاج مسری را محکوم به مرگ می کردند.

Quarantine : برای جلوگیری از انتشار آلودگی فایل های آلوده ای که دو امکان قبلی برای آن ها وجود نداشته است را قرنطینه می کنند.

از آنجا که عدم استفاده از امکانات آنتی ویروس و بی توجهی به پیام های آن پسندیده نیست در اینجا اصطلاحاتی بطور کلی بیان می شود:

Internet security

ابزار جامع امنیتی است که مجموعه بدافزارها و تهدیدات حوزه اینترنت را پوشش می دهد و از آنتی ویروس کامل تر است و شامل : حفاظت فایل ها و حافظه ها - حفاظت ایمیل ها – تهدیدات شبکه و کنترل درگاه های اینترنتی – مقابله با حملات شبکه – فایروال تعبیه شده - و... می باشد.



Virus signature database

نسخه پایگاه داده آنتی ویروس که مربوط به الگوی ویروس های کشف شده است را نشان می دهد و باید به تاریخ جاری بسیار نزدیک باشد.

Update

بروز رسانی نرم افزار یا پایگاه داده آن است و این امکان وجود دارد که خودکار و یا دستی باشد ولی به هر صورت باید بطور مداوم انجام شود.

Infected

فایل هایی که آلوده شده اند.

Threats

تهدیدات کشف شده توسط آنتی ویروس.

Custom or Smart Scan

انتخاب نوع اسکن که انتخابی یا هوشمند باشد.

Log Scan Files

فایلی که گزارش نتیجه عملکرد آنتی ویروس در بررسی فایل ها در آن ذخیره شده است.

Advanced setup Or additional tools

امکات، ابزارها و تنظیمات بیشتر در این قسمت قرار دارد. معمولا نرم افزارها بطور پیشفرض روی حالت بهینه و توصیه شده(Recommended)تنظیم شده اند.

Trusted/Allowed

برنامه یا فایل یا پردازش هایی که مجاز هستند و به انها اطمینان داریم.

Restricted

مواردی که بنابه دلایلی با درجه خاصی محدود شده اند.

Blocked/Denied

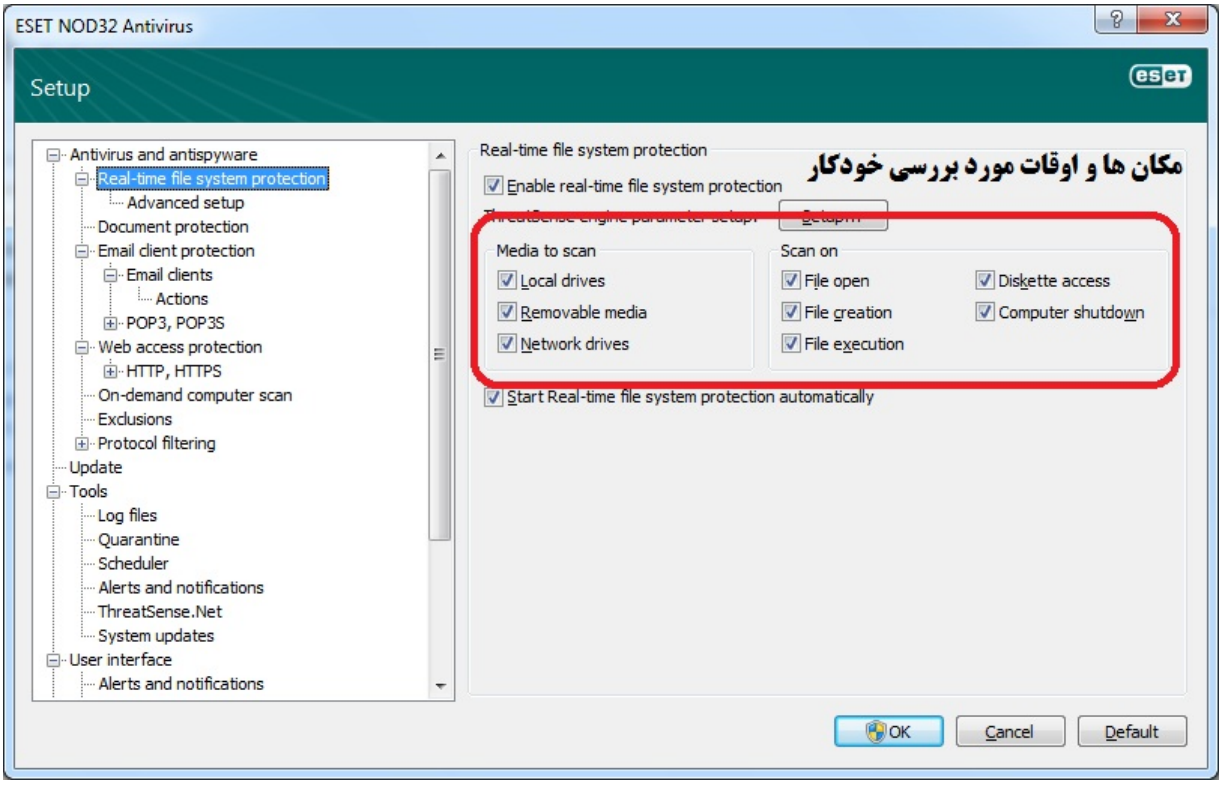
برنامه یا پردازش هایی که بلوکه شده اند و اجازه ندارند.

Create rescue disc

ساختن دیسک نجات که می تواند یک لوح فشرده یا حافظه فلش باشد و اگر وضعیت حادی پیش آید با کمک آن می توانید رایانه را بوت کرده و از آنجا یک اسکن کامل انجام داده از شر ویروس ها خلاص شوید.

Parental Control

برخی از آنتی ویروس ها دارای ابزاری برای کنترل فرزندان توسط والدین هستند مانند محدود کردن زمان استفاده از رایانه و محدود کردن دسترسی به اینترنت، بلوکه کردن برخی سایت ها و ...

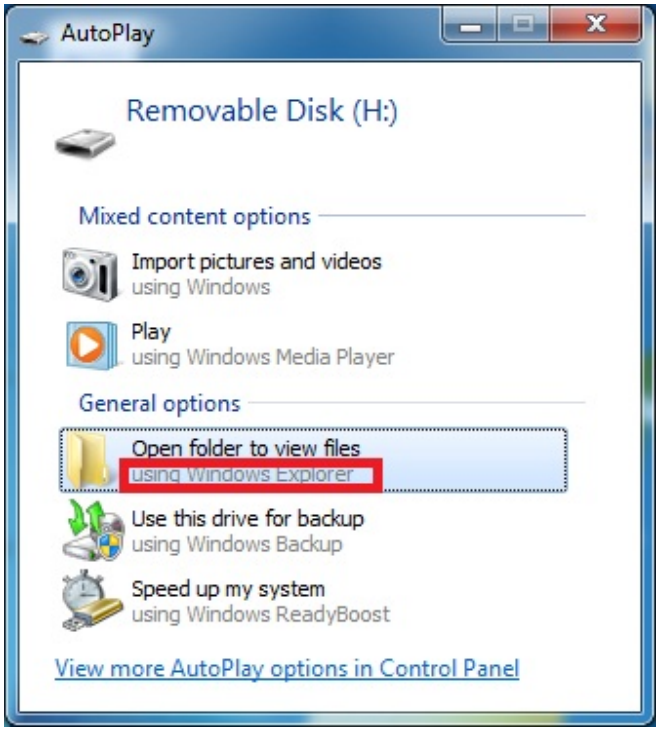


دیواره آتش یا Firewall سخت افزار یا نرم افزاری است که مانند یک حایل رایانه و شبکه شما را از محیط بیرون محافظت می کند.سیستم عامل های ویندوز دارای این امکان هستند که می توانید از آن بهره بگیرید. یک فایروال از شبکه شما در برابر ترافیک ناخواسته و همچنین نفوذ دیگران به رایانه شما حفاظت میکند. توابع اولیه یک فایروال به این صورت هستند که اجازه می دهند ترافیک خوب عبور کند و ترافیک بد را مسدود می کنند! مهمترین قسمت یک فایروال ویژگی کنترل دستیابی آن است که بین ترافیک

خوب و بد تمایز قائل می شود. وقتی آن را نصب می کنید فایروال بین رایانه شما و اینترنت قرار می گیرد. فایروال به شما اجازه می دهد صفحات وب را ببینید و به آن ها دسترسی داشته باشید، فایل دانلود کنید، چت کنید و ... . در حالیکه مطمئن هستید افراد دیگری که در اینترنت مشغول هستند نمی توانند به کامپیوتر شما دست درازی کنند. هر کسی که از اینترنت استفاده می کند باید از بعضی از انواع فایروال ها استفاده کند. برنامه هایی هستند که می توانند از اینترنت دانلود شوند این برنامه ها می توانند تعداد زیادی آدرسهای IP آسیب پذیر برای نفوذ را پیدا کنند، این برنامه ها به راحتی دانلود شده و اجرا می شوند و برای سوء استفاده یا مشکل دار کردن کامپیوتر شما از طریق این برنامه ها احتیاجی به دانش شبکه نیست معمولاً همه انواع فایروالها از شما در برابر این حملات حفاظت می کنند.

ب)استفاده کنترل شده از حافظه فلش

حافظه های فلش به عنوان یکی از پرکاربرترین حافظه های رایانه ای اغلب آلوده به انواع بدافزارها ها هستند بنابراین لازم است حین استفاده از آن ها موارد زیر را در نظر بگیرید



۱- سعی شود قبل از اتصال به رایانه حاوی اطلاعات مهم در یک رایانه دیگر آن را از نظر وجود بدافزارها توسط آنتی ویروس بررسی نمایید.

۲- حالت اجرای خودکار حافظه ها را غیر فعال کرده و هنگام اتصال صرفا گزینه open with windows explorer مانند شکل قبل را انتخاب نمایید .

۳- قبل از باز کردن حافظه فلش آنرا توسط آنتی ویروس بررسی کنید.

٤- برای باز کردن حافظه فلش به جای دابل کلیک روی آن کلیک راست کرده و explore را انتخاب کنید.

٥- از نرم افزارهای مرتبط با حافظه فلش مانند usb disk security استفاده نمایید.

٦- اگر صرفا می خواهید یک فایل را به حافظه فلش منتقل کنید بدون باز کردن آن از گزینه send to removable disk استفاده کنید.

پ)پشتیان گیری از فایل ها و برنامه ها

بسیاری از اوقات مانند مواجهه با یک بدافزار باجگیر راهی بجز استفاده از فایل های پشتیبانی که روی حافظه هایی مانند CD/DVD منتقل کرده اید ندارید بنابراین این اقدام را در اولویت اساسی خود قرار دهید.

ت)استفاده کنترل شده از امکانات اینترنتی

نرم افزارها را از منابع معتبر دریافت کنید، در وبگردی ها مراقب لینک های فریبنده باشید، ایمیل های ناشناس را اصلا باز نکرده و مراقب پیوست آن ها باشید.برای مراجعه به وبسایت ها بجای استفاده از لینک ها، آدرس آن را در نوار آدرس تایپ کنید، در هنگام انجام تراکنش های مالی ضمن توجه به آدرس سامانه به عبارت https و نماد قفل در بالای صفحه، از صفحه کلید مجازی استفاده کنید.

ث)استفاده از حالت کاربری محدود شده به جای حالت کاربری مدیر

بسیاری از اوقات مانند زمان های وبگردی به امکانات دست بالای مدیریتی نیاز ندارید بنابراین از حالت کاربری محدود شده با حداقل دسترسی استفاده کنید چون در این حالت بدافزارها نیز حق دسترسی کمتری دارند؛ همچنین روی حساب های کاربری خود خصوصا با قابلیت های مدیریتی رمز عبور قوی طولانی و ترکیبی از حروف و اعداد که غیر قابل حدث زدن باشد استفاده نمایید. هیچگاه روی همه حساب های خود یک رمز عبور یکسان قرار ندهید چراکه در صورت کشف در یک جا، بقیه حساب های شما هم به خطر می افتد.

ج)محدود سازی دسترسی نامطمئن و از راه دور

به هیچ وجه توصیه نمی شود به کسی به هر نحو امکان اتصال از را دور بدهید؛ روی My Computerخود کلیک راست کرده و Properties را بزنید. حال از منوی سمت چپ گزینه Remote Settingرا انتخاب کرده و تیک جلوی Allow Remote Assistance Connections to this Computer را بردارید.

چ)استفاده از آخرین ورژن نرم افزارهای کاربردی و نصب اصلاحیه های امنیتی

توصیه می شود در صورت انتشار اصلاحیه برای نرم افزارهای کاربردی مانند مجموعه آفیس آن ها را نصب کرده تا راه نفوذی که توسط آسیب پذیری های آن ها بوجود آمده است بسته شود.

ح)امن کردن مرور گرها

تا آنجا که می توانید از نسخه جدید مرورگرها استفاده کنید. اجرای فایل های فلش و اسکریپ ها را روی آن ها غیرفعال کنید؛ هر افزونه ای را روی مرورگر خود نصب نکنید.

خ)بررسی فایل های مشکوک قبل از بازکردن و توجه به پسوند آن ها

پسوند فایل های مهم را بشناسید و به راحتی گول آیکن آن ها را نخورید.

د) بررسی سخت افزار رایانه

یک ضبط کننده سخت افزاری ضربات صفحه کلید، می تواند بطور نامحسوس بین صفحه کلید و رایانه شما قرا بگیرد، پس مراقب باشید. بهتر است وب کم خود را بپوشانید یا آن را جدا کنید.

ر)استفاده کامل و صحیح از روش های بازیابی در هنگام ساخت حساب های آنلاین

اطلاعات بازیابی شامل پرسش محرمانه و ایمیل ثانویه را هنگام ایجاد حساب های کاربری جدی بگیرید.

ز)هوشیاری

به عنوان آخرین راهکار سعی کنید خود را به جای توسعه دهنده بدافزار بگذارید و فکر کنید که یک بدافزار چه چرخه ای را در رایانه شما طی می کند تا با هوشیاری لازم جلوی آن را بگیرید مثلا سناریوی زیر را برای آلودگی به یک باج افزار به عنوان بدترین نوع بدافزارها ارایه می دهیم:

باج افزار باید به نحوی وارد سیستم شما شود که یک راه رایج آن از طریق فریب دادن شما برای دانلود محافظ صفحه نمایش زیبا (مانند آکواریم، نمای زیردریا، رقاص روی میزکار و...) یا باز کردن پیوست ایمیلی ناشناس است؛ خوب این کارها را انجام ندهید!. بعد از ورود، باج افزار باید اجرا شود پس

نباید هر برنامه ای، هرفایل دانلود شده ای را بدون هوشیاری کافی باز کرد و تنظیمات رایانه را طوری تغییر دهید که از اجرای خود بخودی آن جلوگیری شود.بعد از اجرا، باج افزار باید به اینترنت متصل شده و رمز خود را با درگاه اینترنتی خویش هماهنگ کند خوب با فعال کردن فایروال به هر نرم افزاری اجازه دسترسی به اینترنت ندهید. در مرحله بعدی فایل هایی که احتمالا برای شما مهم هستند را احصا می کند(عکس، فایل های آفیس و....)تا در مراحل بعدی آن ها را رمزگذاری کند مراحل اخیر زمان بر و سنگین هستند و شاید بتوانید متوجه آن شوید که در این صورت به هر نحوی که شده رایانه خود را خاموش کرده و با یک متخصص تماس بگیرید؛ البته این گونه ها دائما در حال تغییر هستند و برخی با رصد میزان کارکرد پردازنده بهترین زمان را برای اقدامات خود انتخاب می کنند و مشاهده شده که نمونه ای ازآن ها با علم به اینکه اغلب کاربران بعد از صدور فرمان خاموش کردن رایانه منتظر نمی شوند که واقعا خاموش شود، از خاموش شدن آن جلوگیری کرده و اقدامات خود را انجام می دهند پس همواره سعی کنید از خاموش شدن رایانه خود مطمئن شوید. ابزارهای مقابله با بد افزارها معمولا از رفتار آن ها(دسترسی به اینترنت-عملیات پرحجم احصا،کپی و رمزگذاری)برای شناسایی و مقابله استفاده می کنند. اگر تا این مرحله باج افزار مهار نشود فایل های شما را نابود کرده است پس نسبت به مسائل پشتیبان گیری هوشیار باشید.

نشانه های آلودگی رایانه ها

چگونه بفهمیم که رایانه ما آلوده شده است؟ در پاسخ باید پرسید شما چگونه می فهمید که در میان انبوه امراضی که بشر را تهدید می کند مبتلا به یک بیماری شده اید؟ پاسخ روشن است برخی بیماری ها علایم خاصی دارند، برخی هم بدون علامت می باشند، برخی هم منحصر به سن یا منطقه خاصی هستند، گاهی اوقات هم برحسب شرایطی که در آن قرار گرفته اید احساس خطر می کنید مثلا اگر فردی که به شدت سرفه می کند روبروی شما عطسه کنید احتما می دهید که مبتلا به آنفولانزا خواهید شد؛ لذا بطور مشابه ابتلا به بدافزارهای رایانه ای را در موارد زیر بیان خواهیم کرد:

- اگر بطور مکرر از حافظه های فلش برای مبادله فایل ها استفاده می کنید در خطر ابتلا به کرم های خاص این حالت مخصوصا مخفی شدن فایل های داخل حافظه هستید.
- اگر دنبال دانلود نرم افزارهای کوچک با عملکرد زیاد بوده اید محتمل است آلوده به تروجان ها و ابزار جاسوسی شده باشید.
- اگر از روش های عبور از فیلترینگ استفاده کرده اید بدانید علاوه بر دسترسی ارائه دهنده این روش ها به ترافیک اینترنت شما، ممکن است از رایانه شما به عنوان زامبی استفاده کنند.یعنی رایانه ای که اختیارش دست کاربرش نیست و توسط هکر برای حمله به دیگران و انجام اعمال مجرمانه استفاده می شود.
- اگر با پیام اخطار تقلبی آنتی ویروس مواجه شده اید، پیام های خطری که خیلی ناگهانی روی صفحه مانیتور ظاهر می شود تا به شما بگویند در خطر هستید، همیشه همانی نیستند که به نظر می آید. بعضی از این پیام ها حتی ممکن است از شما برای فعال شدن، درخواست کد فعال سازی بکنند در حالی که بقیه ممکن است از شما بخواهند کلیدی را فشار دهید تا سیستم شما را پاک

کنند. تقریبا تمام پیام های آنلاین از این دست تقلبی هستند و نباید روی آنها کلیک کنید. اما همین که شما این پیام ها را می بینید به این معناست که احتمالا سیستم تان پیشاپیش آلوده شده است.

- **اگر مطالبی ضد صهیونیستی را در اینترنت جست و جو کنید و دقت کافی نداشته باشید مبتلا به ابزار جاسوسی یا ویروس های مختل کننده سیستم خود می شوید.چون از نظر صهیونیست ها شما یا حذب الهی هستید که از شما جاسوسی می کنند و یا از آنجا که بسیار معتقد به آزادی اندیشه هستند! و شما هم صرفا محقق بوده اید باید مجازات شده و رایانه شما از کار بیفتد.**
- **اگر برفرض محال دنبال روش های مجرمانه یا مسایل خلاف اخلاق در اینترنت باشید یا در بررسی و باز کردن ایمیل های ناشناس دقت لازم را مبذول نکنید مبتلا به نوع بسیار خطرناکی از بدافزارها به نام باج افزار شده و واقعا دچار مشکل خواهید شد.**
- **اگر سرعت رایانه شما حین استفاده از نرم افزارهای کاربردی کم شده است و فعالیت پردازنده و گنجایش حافظه رم کمتر از نورم آن باشد می تواند به علت ویروسی بودن رایانه شما باشد.**
- **اگر انجام کارهای ناخواسته ای روی رایانه شما را کلافه کرده و یا سرعت شبکه شما پایین آمده است احتمال رخنه کرم ها در رایانه شما وجود دارد.**
- **اگر بدون ملاحظه آیکن های مشکوکی که روی میز کار شما ظاهر شده اند را بازکنید محتل است که بدافزاری را اجراکرده باشید.**
- **اگر هنگام وب گردی در هنگام تایپ در نوار جستجو، نوار آدرس و... احساس می کنید که کندتر شده است و احتمالا یک تازه سازی خیلی ضعیف در پس زمینه صفحه رخ می دهد احتمالا لاگرها مشغول ثبت عبارات تایپ شده شما هستند.**
- **اگر رایانه شما از لحاظ سخت افزاری ضعیف تر باشد اقدامات بدافزارها در آن نمود بیشتری دارد.**
- **اگر هنوز از سیستم عامل ویندوز XP استفاده می کنید احتمال بیشتری دارد که مبتلا به بدافزارها شوید.**

- **اگر نسبت به اجرای تمهیدات امنیتی روی رایانه خود بی تفاوت بوده اید واحساس می کنید در حساب های کاربری سیستم عامل شما تغییر به وجود آمده مثلا قبلا حساب administrator قابل مشاهد نبوده ولی اکنون هست احتمالا هکر یک درپشتی برای ورود خود به رایانه شما باز کرده است.**
- **اگر هرزنامه ارسال شده به ایمیل خود را باز کنید مستعد ارسال بیشترین حجم هرزنامه ها خواهید شد.**
- **اگر اجازه اتصال از راه دور به کسی داده باشید ممکن است هرنرم افزاری نصب کرده باشد و هر تنظیمی اعمال کرده باشد.**
- **اگر نکات امنیتی را پیرامون مرورگرها رعایت نکرده باشید مستعد شنود و دریافت تبلیغات مزاحم و آزاردهنده هستید.**
- **اگر انواع برنامه های موبایل را بدون ملاحظه روی گوشی همراه خود نصب می کنید گوشی خود را در معرض انواع تروجان ها قرار داده و برای اطلاعات و حریم شخصی خود ارزشی قایل نشده اید.**
- **اگر پیام های صادره هنگام نصب برنامه های رایانه ای یا اپلیکیشن های موبایل را نخوانده تایید می کنید به آن ها دسترسی غیر مجاز داده و امنیت خود را به مخاطره انداخته اید، به همین علت است که بیشترین تهدید پیرامون حوزه تلفن همراه در کشور ریسک افزارها هستند.**
- **اگر به اشتباه پاسخ یکی از پیامک های تبلیغاتی و تجاری که واقعا گول زننده هستند را بدهید علاوه بر ایجاد مزاحمت بیشتر برای شما، هزینه تبلیغ هم از جیب شما پرداخت خواهد شد که به آن تروجان پیامکی می گویند.**
- **اگر برخی امکانات رایانه شما از کار افتاده است مثلا در صورت از کار افتادن Task Manager وMsconfig ، از کار افتادن آنتی ویروس، در صورت دیدن علایم مشکوک در مسنجر، فعال بودن**

نرم افزارهای مشکوک، مثل Task Manager وMsconfig و خوانده شدن ایمیل هایی که قبلا آن ها را در ایمیل خود نخوانده اید با تروجان ها سروکار دارید.

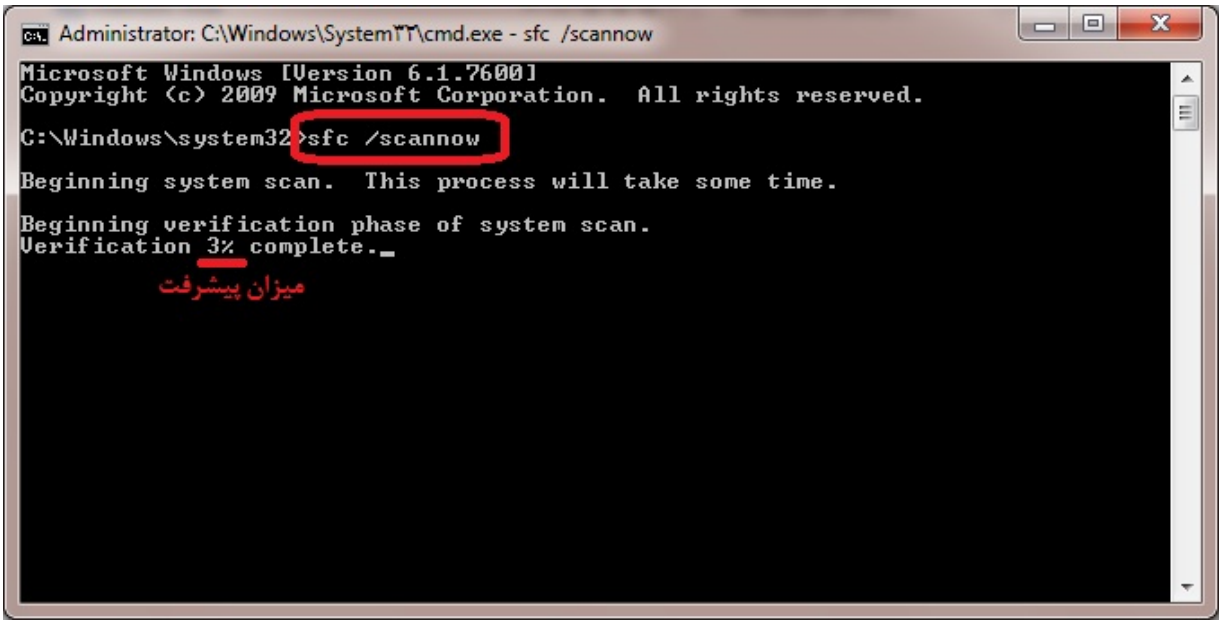
- اگر بدانید که یکی از روشهای آلوده شدن بهSpyware ، نصب همزمان آن با برنامه های دیگری است که شما واقعا قصد نصب آن ها را ندارید، مثل برنامه های به اشتراک گذاری فیلم یاموسیقی. هرزمان که برنامه ای را نصب می کنید مطمئن می شوید که تمام موافقت نامه های مرتبط و همچنین مستندات آن نرم افزار را به دقت مطالعه کرده اید.
- اگر آگهی های تبلیغاتی را در تمام مدت مشاهده می کنید بدانید که به احتمال زیاد آلوده به Spyware هستید.
- اگر تنظیمات رایانه شما تغییر کرده و نمی توانید آن را به حالت اولیه خود برگردانید مثلا صفحه خانگی مرورگر شما تغییر کرده، نرم افزارها و ابزارهایی در مرورگر شما نصب شده که از آن اطلاعی ندارید و نمی توانید آن ها را حذف کنید احتمالا ابزارهای جاسوسی در رایانه شما لانه کرده اند.
- اگر احساس می کنید حجم فایل های اجرایی شما زیادتر شده شاید یک ویروس خود را به آن الصاق کرده باشد.
- اگر برنامه هایی که اجرایشان می کنید بدرستی اجرا نمی شوند و با چند پیغام خطا که برایتان تازگی دارند از ادامه کار باز می ماند. این می تواند علامت رونویسی کد توسط یک ویروس باشد
- اگر تغییرات مشکوکی در پوشه ها مشاهده می کنید و متوجه می شوید که حین اجرای یک برنامه به یک پوشه دیگر انتقال یافته اید احتمالا یک ویروس شروع به شکار فایل ها در پوشه برنامه شما کرده است.
- اگر پیغام های غیر معمولی از طرف آنتی ویروس خود دریافت می کنید ممکن است پیام تقلبی و شبیه سازی شده باشد. در صورتی که آنتی ویروس شما این پیغام را نفرستاده است روی هیچ چیز کلیک نکنید و اقدامات واکنش سریع را که بعدا گفته می شوید انجام دهید.

- **اگر در حال کار کردن با رایانه به شرط اطمینان از سالم بودن موس متوجه حرکت غیر منتظره نشانگر موس شده اید شاید توسط یک هکر حرفه ای هک شده باشید.**
- **اگر چراغ وب کم شما خود به خود روشن و خاموش میشود. متاسفانه دچار یکی از انواع رایج هک شده اید و یک نفر تصویر شما را بدون اجازه مشاهده می کند.**
- **اگر...**

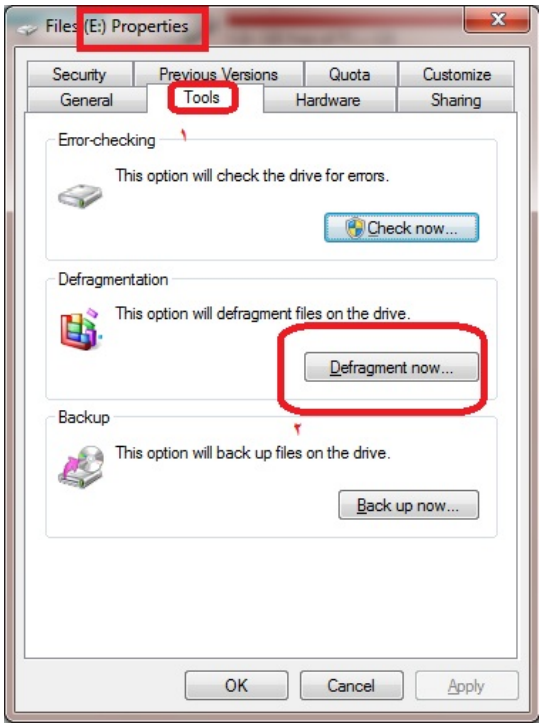
توهم ویروسی شدن

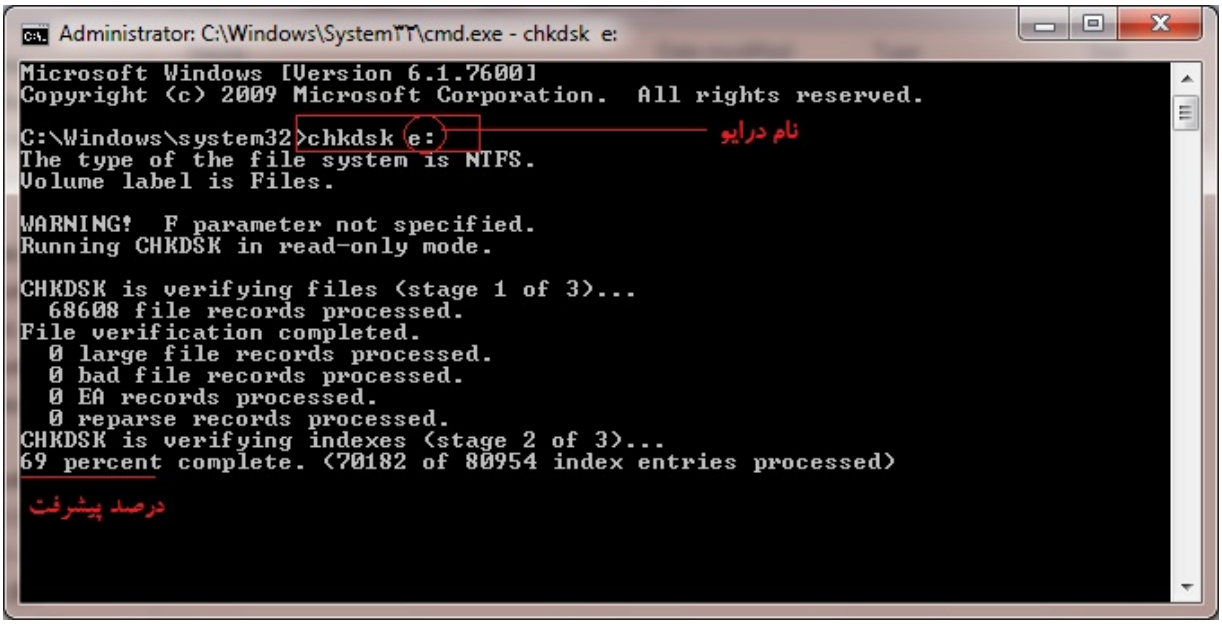
حتما برای شما پیش آمده که علایمی مانند سرفه و گلودرد داشته باشید و پیش خود احتمال دهید که دچار سرما خوردگی شده اید ولی در واقع حساسیت فصلی یا رفلاکس معده باعث بروز چنین علائمی در شما شده باشد؛ برای رایانه ها هم ممکن است همین اتفاق رخ بدهد یعنی ممکن است موارد مذکور بالا در رایانه شما به جای ابتلاء به بدافزار نشانه ای از موارد زیر باشد:

- **مشکلات سخت افزاری و عدم انطباق برخی سخت افزارها با یکدیگر: این حالت معمولا زمانی اتفاق می افتد که تغییری در سخت افزار رایانه خود داده یا وسیله جدیدی را به کیس رایانه خود متصل کرده باشید، شاید هم یکی از سخت افزارهای رایانه شما مستعمل شده باشد و بدرستی کار نکند و نویز تولید نماید. حواستان به پریز و محافظ برق و تغذیه رایانه تان باشد.**
- **مشکلات نرم افزاری: اگر علایم ویروسی شدن رایانه پس از نصب نرم افزار جدید یا اعمال تنظیمات نرم فزاری خاصی باشد احتمالا باز خبری از بدافزارها نیست؛ گاهی اوقات فایل های سیستم عامل باید تازه سازی شوند که استفاده از دیسک مربوط به سیستم عامل و دستور sfc /scannow می تواند به رفع مشکل کمک نماید.**



- مشکلات حافظه: به مرور زمان حافظه رایانه بهم ریخته می شود و ممکن است کارایی لازم خود را از دست بدهد، در این حالت از عملیات defragmentation و دستور chkdsk استفاده کنید.





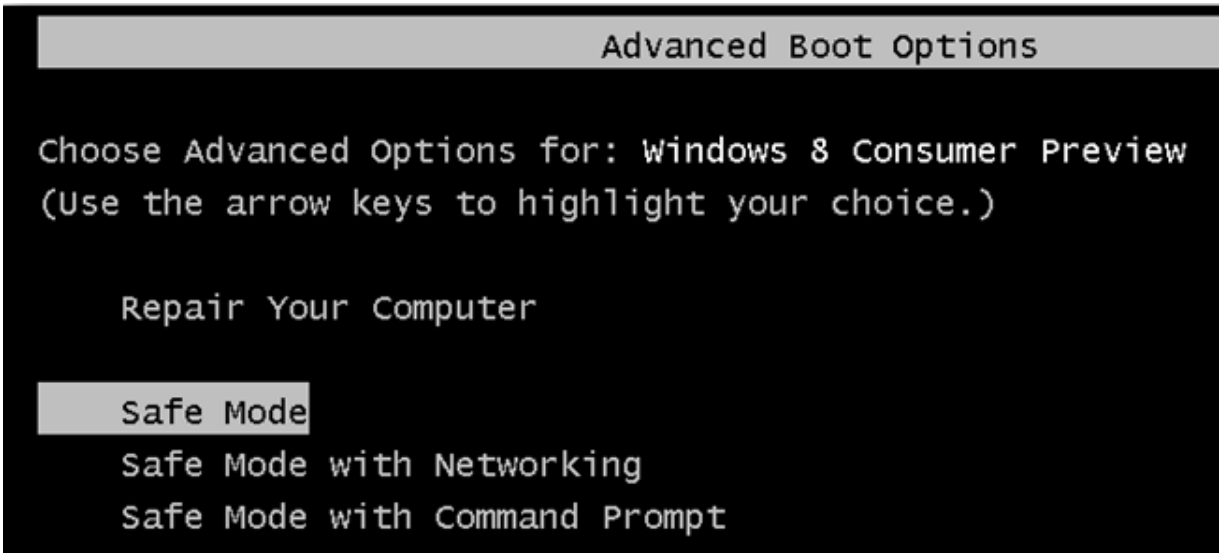
- شرایط آب و هوایی و مکانی: بله درست شنیدید آب و هوا در عملکرد رایانه شما موثر است. بدانید که گرد و خاک، گرما و رطوبت دشمن رایانه شما هستند و در تولید الکتریسیته ساکن و اختلال در تغذیه دستگاه ها موثرند؛ اگر یک قطره آب درون صفحه کلید رایانه شما بریزد ممکن است چنان اتصالی بکند که خیال کنید کنترل رایانه تان از دست شما خارج شده است!. در مورد شرایط مکانی مثلا در اطراف یک سیم برق لخت میدان مغناطیسی وجود دارد که می تواند روی عملکرد سخت افزار رایانه شما مثل صفحه نمایش یا مودم تاثیر بگذارد؛ لپ تاپ خود من اگر هنگام رایت کردن سی دی روی زمین سفت باشد سی دی را با خطاهای عجیبی می سوزاند ولی اگر روی میز لرزانی باشد مشکلی پیش نمی آید.

مقابله با بدافزارها

اگر مرحله پیشگیری را بخوبی طی کرده باشید به ندرت وارد این مرحله می شوید ولی گاهی اوقات ناچارید که

اقدامات ذیل را به عنوان واکنش سریع انجام دهید :

- **قطع ارتباط با اینترنت.**
- **خاموش کردن رایانه و تماس با متخصص حسب مورد.**
- **با استفاده از گوشی یا هر رایانه دیگری که مطمئن هستید پاک است، به سرعت پسورد تمامی اکانت های خود را تغییر دهید و اگر نمی توانید سریعا از بازیابی پسورد استفاده کنید.**
- **رایانه آلوده را در وضعیت Safe Mode روشن کرده و با استفاده از آنتی ویروس آن را اسکن کنید.**
- **از دیسک نجاتی که قبلا ایجاد کرده اید استفاده کنید.**
- **نرم افزارها، فایل ها و پوشه های مشکوک را پاک کنید.**



اسکن کاملی روی رایانه خود انجام داده و فایل های آلوده شناسایی شده را از طریق آنتی ویروس پاک کنید.

اطلاع از مسیر بدافزارها و ویروس های پیدا شده می تواند به یافتن ریشه آلودگی و جلوگیری از رخداد مجدد آن کمک کند. دانلود برخی فایل ها ، مراجعه به بعضی درگاه و نصب برخی نرم افزارها هرگز نباید دوباره تکرار شود.

ویندوز خود را عوض نموده و تنظیمات جدیدی اعمال نمایید.

فلش آلوده خود را فرمت کنید.

فایل های پشتیبان و تنظیمات ذخیره شده قبلی را بازیابی کنید.


امام سید
علی