در مقالات قبل در مورد نحوهٔ نصب ویندوز و درایورها و نرم‌افزارهای عمومی صحبت کردیم. اما به نظر می‌رسد در مورد یک دسته از نرم‌افزارهای مهم که همان برنامه‌های امنیتی هستند صحبت نکردیم. دلیل آن هم، اهمیت این دسته از نرم‌افزارهاست که به توضیحات جامع‌تری نسبت به دیگر نرم‌افزارها نیاز دارند.

برنامه‌های مخرب[1] برنامه‌هایی هستند که به نحوی به رایانه آسیب وارد می‌کنند. مثلاً رایانه را کند یا داده‌ها را آلوده و خراب می‌کنند. براساس نوع فعالیت، می‌توان این برنامه‌ها را به انواعی مثل ویروس‌ها، کرم‌ها[2]، اسب‌های تروا[3]، برنامه‌های جاسوسی و غیره تقسیم کرد.

سؤال این است که چگونه می‌توان رایانه را در مقابل این نرم‌افزارهای مخرب بیمه کرد و از شر آسیب‌های آن‌ها در امان ماند. جا دارد نکتهٔ بسیار مهمی را که بسیاری از کاربران به آن دقت نمی‌کنند تذکر دهیم. دوستان عزیز باید دقت داشت، با توجه به پیشرفت روزافزون فناوری اطلاعات و تبدیل آن به خدمتی عادی، حتی در بسیاری از مراکز دولتی نظیر بانک‌ها یا مؤسسات، و انجام بسیاری از فرایندهای پراهمیت نظیر انجام امور بانکی روی سیستم خود، باید بسیار بیش از گذشته نسبت به امنیت دستگاه خود حساس باشید. برای مثال گاه برنامه‌های مخرب می‌تواند بسیاری از مطالب مهم رایانه، نظیر رمز عبور حساب بانکی شما که آن را با صفحه کلید تایپ می‌کنید در فایلی ضبط و در اختیار هکرها قرار دهد.

مثال دیگر آنکه با پیشرفت نسل دوربین‌های دیجیتال، امروزه بسیاری از مردم از این وسایل برای عکاسی استفاده می‌کنند و اطلاعات شخصی خود را روی رایانهٔ خود ذخیره می‌کنند. حال اگر رایانه امنیت کافی نداشته باشد امکان هک شدن سیستم شما و برداشتن این اطلاعات و قرار گرفتن آن‌ها در معرض دید همگان در شبکهٔ جهانی اینترنت فراهم خواهد شد. برای مثال آخر تصور کنید مدت زیادی را برای جمع‌آوری اطلاعاتی صرف کرده‌اید یا مثلاً حدود یک ماه را برای تایپ پایان‌نامه و نظایر آن وقت گذاشته‌اید، حال با ویروسی شدن رایانه‌تان کل اطلاعات شما پاک خواهد شد. با توجه به مثال‌های فوق، اهمیت حفاظت از رایانه را بیش از پیش می‌توان درک کرد.

توصیهٔ ما برای حفاظت از رایانه، نصب سه نرم‌افزار به صورت همزمان است. البته پر بدیهی است که اگر امکان نصب هر سه نرم‌افزار وجود ندارد توصیهٔ مؤکد است که حتماً یک نرم‌افزار بستهٔ جامع امنیتی نصب کنید.

برنامه‌های مخرب می‌تواند بسیاری از مطالب مهم رایانه، نظیر رمز عبور حساب بانکی شما که آن را با صفحه کلید تایپ می‌کنید در فایلی ضبط و در اختیار هکرها قرار دهد

DOWNLOAD

نرم‌افزار اول: آنتی‌ویروس یا بستهٔ جامع امنیتی

در این قسمت شما باید از یکی از نرم‌افزارهای آنتی‌ویروس یا برنامه‌های جامع امنیتی استفاده کنید. در مورد آنتی‌ویروس‌ها در نظر گرفتن چند نکته ضروری است. آنتی‌ویروس‌ها معمولاً سرعت رایانه را به شدت کاهش می‌دهند. بعضاً تنظیمات پیچیده دارند و کاربر را دچار پریشانی می‌کنند. البته بعضی از آنتی‌ویروس‌ها هم حساسیت بسیار بالایی دارند و هنگام کار روزانه، کاربر را اذیت می‌کنند. از طرف دیگر باید حتماً به‌روز شوند؛ با توجه به تولید ویروس‌های جدید، آنتی‌ویروسی که به‌روز نشود خیلی مؤثر نخواهد بود. لذا باید در انتخاب آن دقت کرد. در این مقاله فرصت کافی برای مقایسهٔ آنتی‌ویروس‌ها نداریم و فقط براساس تجربه‌ای قابل دفاع، استفاده از نرم‌افزار Eset Smart Security را توصیه می‌کنیم که قدرت قابل قبول، سرعت مناسب و راهبری نسبتاً آسانی دارد. شما می‌توانید آن را از نشانی زیر دریافت کنید:

dl.softgozar.com/Files/Software/ESET_Smart_Security_Business_Edition_4,2,76,0_x86_Soft-gozar.com.exe

در مورد این آنتی‌ویروس نکتهٔ قابل توجه این است که امکان به‌روزرسانی آن، هم به صورت آن‌لاین (هنگام اتصال به اینترنت) و هم به صورت آفلاین (هنگام نداشتن اتصال به اینترنت) مهیا شده است که هم در پایگاه اینترنتی بالا و هم در مستند موجود در نشانی زیر، آموزش نحوهٔ انجام آن قابل دسترس است:

mobincenter.net/Images/BookFiles/11.zip

سارق

امروزه بسیاری از مردم از دوربین‌های دیجیتال برای عکاسی استفاده می‌کنند و اطلاعات شخصی خود را روی رایانهٔ خود ذخیره می‌کنند. حال اگر رایانه امنیت کافی نداشته باشد امکان هک شدن سیستم شما و برداشتن این اطلاعات و قرار گرفتن آن‌ها در معرض دید همگان در شبکهٔ جهانی اینترنت فراهم خواهد شد

DOWNLOAD

نرم‌افزار دوم: نرم‌افزار تخصصی برای گرفتن برنامه‌های مخرب فلش

با توجه به افزایش استفادهٔ روزانه از فلش‌مموری‌ها[4] و تسهیل انتقال ویروس‌ها و برنامه‌های مشابه از طریق این وسایل، توصیهٔ ما به شـــما عزیزان، استفاده از نرم‌افزاری تخصصی برای بررسی این‌گونه حافظه‌هاست (کلیهٔ وسایلی که با درگاه USB به رایانه متصل می‌شـــوند، نظیر فلش‌مموری، هاردهای خارجی یا اکسترنال و موارد مشابه). لذا استفاده از نرم‌افزار USB Disk Security را به شما عزیزان پیشنهاد می‌کنیم. شما می‌توانید نسخهٔ ۶ آن را از نشانی زیر دریافت کنید:

dl.softgozar.com/Files/Software/USB_Disk_Security_6,1,0,432_AI_Softgozar.com.exe

DOWNLOAD

نرم‌افزار سوم: نرم‌افزاری برای مقابلهٔ بیشتر با حملهٔ هکرها

با توجه به استفادهٔ زیاد از اینترنت، احتمال آلوده شدن ویندوز به تروجان‌ها و موارد مشابه که امکان سرقت اطلاعات را برای هکرها فراهم می‌آورد توصیه می‌شود. از برنامهٔ تخصصی زیر برای مقابله با این‌گونه حملات استفاده کنید. اگرچه این برنامه تا حدی کار آنتی‌ویروس را هم انجام می‌دهد، ولی ما نصب این نرم‌افزار را برای مقابلهٔ بهتر با بدافزارها و حملات هکرها پیشنهاد می‌کنیم:

dl.softgozar.com/Files/Software/Malwarebytes_Anti-Malware_1,62,0,1300_Softgozar.com.exe

نصب هر سه نرم‌افزار گفته شده در کنار یکدیگر تست شده و علاوه بر آن‌که امنیت قابل توجهی برای رایانهٔ شـــما به ارمغان می‌آورد، آن را، آنچنان که ملموس باشد، کند نمی‌کند. در حالی‌که این ایراد به بسیاری از آنتی‌ویروس‌ها وارد است.

در پایان قصد داریـــم به قاعده‌ای طلایی بـــرای تأمین امنیـــت رایانه‌تان اشاره کنیم: همواره برنامه‌های مخرب، با سطح دسترسی کاربر جاری در سیستم فعالیت می‌کنند. به بیان دیگر، همان‌طور که احتمالاً بسیاری از شما عزیزان می‌دانید، ما دو سطح دسترسی کلان در ویندوز داریم: ۱. مدیر سیســـتم؛ ۲. کاربر محدود. اگر شـــما با ســـطح دسترسی مدیر سیســـتم در رایانهٔ خود مشغول به کار باشـــید، احتمال آلوده شدن سیستم شـــما به مراتب بسیار بیشتر از این است که با سطح دسترســـی کاربر محدود در ویندوز مشـــغول کار باشـــید، زیرا کاربر محدود اجازهٔ نصـــب نرم‌افزار و اضافه یا کم کردن اطلاعات پوشه و درایو ویندوز شما را ندارد. اگر شما با این سطح دسترســـی دچار ویروس یا موارد مشابه شـــوید، رایانه‌تان بســـیار کمتر از حالت عادی دچار مشـــکل خواهد شد. تا پایان این مقاله ما رایانه‌ای پاک و خوب برای کار در فضای مجازی داریم و از مقالهٔ بعد بایـــد به بعضی از قابلیت‌های این فضا و نحوهٔ درست کار با آن‌ها اشاره کنیم.

پی‌نوشت
1. Malwares
2. worms
3. Trojans
4. Flash Memory

ـان اطـــلاعـــات

آرمان صوفیانی