آموزش برنامهٔ Windows Defender

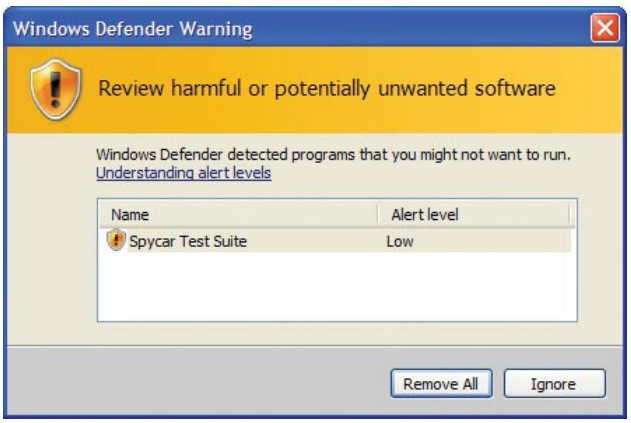
اگر از اینترنت استفاده می‌کنید، اطلاعات و کامپیوترتان در معرض خطر است. البته، عبور از خیابان هم بی‌خطر نیست. حتی پرداخت صورت‌حساب‌ها از طریق پست به مجرمان امکان می‌دهد که اطلاعات شخصی شما را پیدا کنند. همچنان که نمی‌توانیم به شما توصیه کنیم که از خیابان عبور نکنید، یا بدهی‌های خود را پرداخت نکنید، نمی‌توانیم توصیه کنیم که از اینترنت استفاده نکنید.

نرم‌افزارهای ایمن‌ساز به شما کمک می‌کنند که خطرات اینترنت را به حداقل برسانید. اکثر کاربران از گونه‌ای از نرم‌افزار ضدویروس بهره می‌گیرند، اما برنامهٔ ضدویروس به تنهایی دیگر کافی نیست. با آن که شاید **پایش‌افزار**[1] به اندازهٔ یک ویروس مخرب نباشد، انواع دیگری از مسائل را می‌تواند به وجود بیاورد، از آهسته‌کردن کامپیوتر تا ارسال اطلاعات خصوصی شما به اشخاص ثالث، نمایش آگهی‌های بازرگانی بر روی کامپیوترتان به هنگامی که به اینترنت وصل نیستید، و حتی تغییردادن بدون اجازهٔ تنظیم‌های سیستم‌تان. امروزه، بسیاری از مجموعه‌های نرم‌افزاری ایمن‌سازی (مانند Norton Internet Security[2]، McAfee Internet Security[3] و Grisoft AVG Anti-Virus[4]) علاوه بر برنامهٔ ضدویروس حاوی برنامهٔ ضدپایش‌افزار و سایر برنامه‌های ایمن‌سازی هستند. اما اگر یک برنامهٔ ضدویروس مستقل را اجرا می‌کنید باید برای کامپیوترتان حفاظت کافی در برابرپایش‌افزارها را نیز به وجود بیاورید.

اگر مدتی یک کاربر ویندوز بوده باشید، حتماً چیزهایی دربارهٔ خطرات **پایش‌افزار** یا **برنامه‌های جاسوسی** می‌دانید. این روزها، چنین به نظر می‌رسدکه یک پایش‌افزار پشت هر صفحهٔ وبی، ایمیلی، یا فایل دریافتی‌ای[5] پنهان شده است. برای مبارزه با بلای پایش‌افزار، تعداد زیادی **برنامهٔ ضدپایش‌افزار**[6] به بازار عرضه شده است. مایکروسافت هم بیکار ننشست و محصول خود را به نام **Windows Defender** ارائه کرد.

برنامهٔ Windows Defender به منظور شناسایی و حذف پایش‌افزار موجود، و همچنین جلوگیری از آلودگی جدید طراحی شده است و با زیرنظرگرفتن سیستم از لحاظ فعالیت‌های مشکوک وظیفهٔ خود را انجام می‌دهد.

برنامهٔ رایگان Windows Defender مایکروسافت برای کاربران **ویندوز اکس‌پی، ویستا، و ویندوز۷** یک حفاظ در برابر پایش‌افزارها برپا می‌سازد. در این مقاله به شما نشان خواهیم داد که چگونه از Windows Defender برای حفاظت کامپیوترتان استفاده کنید.

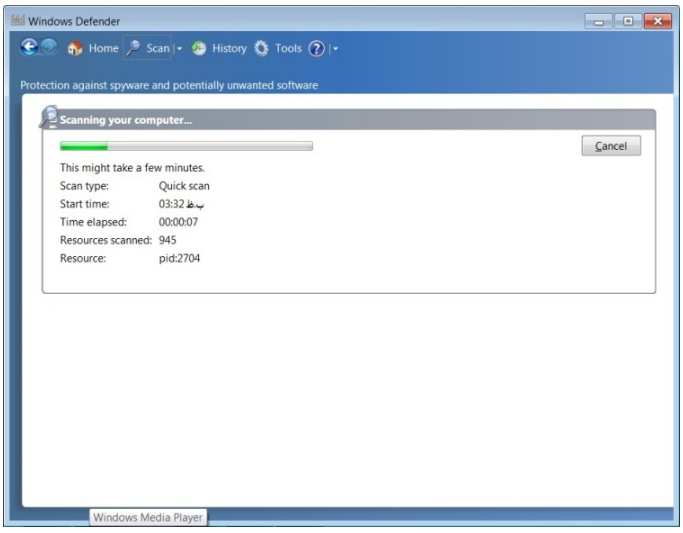


حفاظت پیوستهٔ Windows Defender، اگر هر فعالیت مسئله‌داری را در سیستم شما تشخیص بدهد به طور خودکار به اطلاع شما می‌رساند.

سیستم خود را بررسی کنید

برای اجرای دستی برنامهٔ Windows Defender، در کادر Search در منوی Start ، کلمهٔ defender را تایپ کنید و کلید Enter را بزنید.

سپس، برای بررسی سریع، روی پیکان رو به پایین در کنار Scan کلیک کنید و Quick Scan را انتخاب کنید. برنامهٔ Windows Defender سیستم شما را مورد بررسی قرار می‌دهد. این بررسی سریع به چند ناحیه‌ای محدود می‌شود که احتمال آلوده‌بودن آنها بیشتر است، اما بر روی بعضی از سیستم‌ها، حتی یک بررسی سریع می‌تواند مدتی طول بکشد.



[1] spyware
[2] http://www.symantec.com/
[3] http://www.mcafee.com/
[4] http://www.avg.com/
[5] downloaded file
[6] antispyware

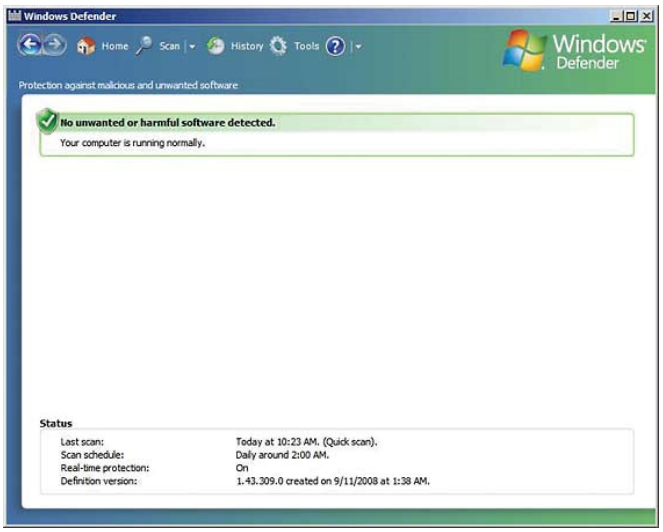
برای اجرای یک بررسی کامل از دیسک سخت خود، روی پیکان رو به پایین در کنار Scan کلیک کنید و Full Scan را انتخاب کنید. اگر یک بررسی در مورد فایل‌های ویژه را بخواهید به اجرا درآورید، گزینهٔ Custom Scan را انتخاب کنید. اگر Windows Defender یک برنامهٔ جاسوسی یا نرم‌افزار مشکوک را بیابد، اطلاعاتی دربارهٔ هر مورد به نمایش در خواهد آورد، شامل شرح و مکان آن نرم‌افزار، یک سطح هشدار، و یک عمل مورد توصیه.

پنج سطح هشدار وجود دارد: Not Yet Classified، Low، Medium، High، و Severe. هر چیزی با یک سطح هشدار High یا Severe باید حذف شود، مگر این که به برنامه اعتماد داشته باشید. اگر مطمئن باشید که برنامه درست است، می‌توانید Always Allow را انتخاب کنید، تا Windows Defender دیگر آن را دوباره علامت‌گذاری نکند. اگر مطمئن نباشید، می‌توانید Quarantine را انتخاب کنید، که آن نرم‌افزار را غیرفعال خواهد کرد. پس از آن که Windows Defender نرم‌افزار مضر را حذف کرد، از شما ممکن است بخواهد که کامپیوتر را بازراه‌اندازی کنید.

برنامهٔ Defender، همچنین با تحت‌نظرگرفتن سیستم از لحاظ تغییرات در فایل‌های اساسی یا تنظیم‌های مهم، یک حفاظت پیوسته را نیز به وجود می‌آورد. اگر چنین تغییراتی تشخیص داده شود، Windows Defender یک پنجرهٔ هشدار به نمایش در خواهد آورد که به شما امکان می‌دهد برنامهٔ مهاجم را حذف کنید.

جنگ را آغاز کنید

Windows Defender پس از بررسی اولیه، شما را به صفحهٔ Home باز خواهد گرداند. در اینجا، حالت فعلی کامپیوتر خود را می‌توانید ببینید، و در پایین این صفحه، یک گزارش وضعیت، شامل تاریخ روز و ساعت آخرین بررسی به نمایش در می‌آید.



مبانی. Windows Defender همچون یک برنامهٔ ضدویروس، فایل‌های در دست بررسی خود را با یک **فایل رمز مشخصه** مقایسه می‌کند که مایکروسافت آن را به طور منظم روزآمد می‌کند. اگر Windows Defender در مقایسه‌های خود یک همسانی را بیابد، یا عملیات ازپیش‌طراحی‌شدهٔ خود را انجام می‌دهد، یا از شما می‌خواهد که مشخص کنید بر سر فایل مظنون چه باید آورد. مایکروسافت پایش‌افزار را در یکی از پنج Alert Levels گروه‌بندی می‌کند: Severe، High، Medium، Low، و Not Yet Classified.

پایش‌افزار یک اصطلاح دارای یک تعریف روشن نیست. به عنوان مثال، یک برنامه را فقط به این دلیل که تنظیم‌های سیستمی را تغییر می‌دهد نمی‌توان در شمار **برنامه‌های داده‌ستیز** قرار داد. در نتیجه، Windows Defender گاهی ممکن است برنامه‌های مفید را به عنوان پایش‌افزار شناسایی کند. هرگاه چنین اتفاقی روی بدهد، می‌توانید گزینهٔ Ignore را انتخاب کنید، که در این صورت Windows Defender در هر زمان که یک بررسی را انجام می‌دهد به هشداردادن خود در مورد این برنامه ادامه خواهد داد، یا می‌توانید برنامه را در فهرست Allowed Items اضافه کنید تا Windows Defender دیگر

نرم‌افزارهای مشابه بازار

همچنان که پیشتر ذکر کردیم، بسیاری از مجموعه‌های نرم‌افزاری ایمن‌سازی در کنار برنامه‌های ضدویروس و ابزار امنیتی دیگر خود یک برنامهٔ ضدپایش‌افزار دارند. حال اگر از قبل یک برنامهٔ ضدپایش‌افزار نصب کرده باشید آیا نصب و اجرای Windows Defender فایده‌ای دارد؟

یک سخنگوی مایکروسافت می‌گوید که بعضی از کاربران ممکن است از اجرای چند برنامهٔ ضدپایش‌افزار منتفع بشوند، اما هزینهٔ آن مصرف بیشتر **منابع سیستم** است. افزون بر این، همیشه مشخص نیست که چقدر برای کاربر فایده خواهد داشت. تا اندازهٔ زیادی به نحوهٔ تعریف برنامهٔ ضدپایش‌افزار از پایش‌افزار بستگی دارد.

اگر برنامه‌های ضدپایش‌افزاری‌ای را بیابید که مکمل همدیگر باشند اجرای چند برنامهٔ ضدپایش‌افزار می‌تواند مفید باشد، در غیر این صورت، نصب چند برنامه ارزشی ندارد. اگر چند برنامه نصب شود احتمال نتایج **مثبت نادرست** (false positive) زیاد می‌شود، که می‌تواند بر ابهامات کاربر اضافه کند. به عنوان مثال، شرکت AVG مدعی است که برنامهٔ AVG Anti-Virus با برنامه‌های دیگر ضدپایش‌افزار تداخل ندارد، اما این شرکت اجرای AVG را در کنار برنامه‌های دیگر ضدپایش‌افزار و ضدویروس توصیه نمی‌کند.

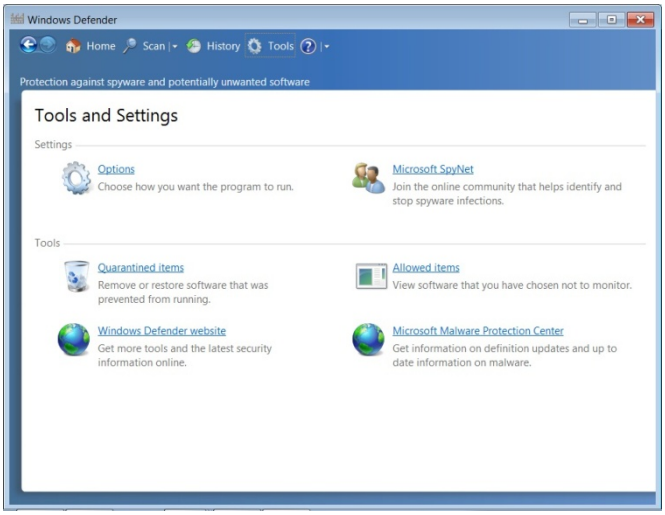
توصیهٔ ما آن است که یک برنامهٔ ضدپایش‌افزار خوب پیدا کنید و فقط از همان برنامه استفاده کنید.□

آن فایل را تحت نظر نگیرد.

همچنین، برای پایش‌افزارهای پیداشده می‌توانید گزینه‌های Quarantine یا Remove را انتخاب کنید. Quarantine چنین فایلی را به یک دیرکتوری متفاوت انتقال می‌دهد و جلوی اجراشدن آن را تا زمانی می‌گیرد که شما آن را آزاد کنید. گزینهٔ Remove، پایش‌افزار یافته‌شده، یا برنامه‌های افزوده‌شده به فهرست Quarantine را حذف می‌کند.

زمان بررسی. Windows Defender دو سطح از بررسی را فراهم می‌سازد. **Quick Scan** فقط پوشه‌هایی را بررسی می‌کند که احتمال وجود پایش‌افزار در آنها هست، در حالی که **Full Scan** کل دیسک‌سخت را بررسی می‌کند. به هنگام عملیات بررسی ممکن است کامپیوتر آهسته شود. در نتیجه، مایکروسافت توصیه می‌کند که فقط وقتی Full Scan را به اجرا درآورید که معتقدید یک مسئلهٔ پایش‌افزاری در کامپیوتر به وجود آمده است.

به طور پیش‌فرض، Windows Defender طوری میزان می‌شود که یک Quick Scan را هر بامداد ساعت ۲ به اجرا درآورد. برای تغییردادن ساعت یا تعداد بررسی، روی Tools و بعد Options کلیک کنید.



در اینجا همچنین می‌توانید واکنش‌های پیش‌فرض Windows Defender را برای زمانی که یک پایش‌افزار را می‌یابد میزان کنید؛ واکنش‌ها در یکی از گروه‌های High، Medium، یا Low جای می‌گیرد. به طور پیش‌فرض، Windows Defender مطابق دستورالعمل مشخص‌شده در فایل رمز مشخصه عمل می‌کند. ما توصیه می‌کنیم با تنظیم‌های پیش‌فرض کار کنید، اما می‌توانید یکی از گزینه‌های Ignore، Quarantine، یا Remove را برای فایل‌های شناسایی‌شده انتخاب کنید.

وصله‌های روزآمدساز. اگر از یک فایل **رمز مشخصهٔ** تاریخ‌گذشته استفاده می‌کنید بررسی پایش‌افزار در کامپیوتر بر اساس یک جدول زمان‌بندی حفاظت خوبی ایجاد نمی‌کند. با آن که Windows Defender فایل‌های رمز مشخصهٔ جدید را از طریق Windows Update دریافت می‌کند، مایکروسافت توصیه می‌کند که Windows Defender را طوری میزان کنید که پیش از هر بررسی خود ابتدا به بررسی وجود فایل‌های رمز مشخصهٔ جدید بپردازد. باید مربع کنار عبارت Check For Updated Definitions Before Scanning در بخش Options تیک‌دار باشد. اگر ترجیح می‌دهید فایل رمز مشخصه را به طور دستی روزآمد کنید، روی دکمهٔ پیکانی Down در کنار آیکن Help کلیک کنید. سپس، روی Check For Updates کلیک کنید. مایکروسافت اگر فایل‌های رمز مشخصهٔ شما بیش از هفت روز عمر داشته باشند به شما هشدار خواهد داد.

تنظیم به سلیقهٔ خودتان

روی Tools و Options کلیک کنید. نوع بررسی را مشخص و یک جدول زمان‌بندی برپا کنید. همچنین می‌توانید برنامهٔ Defender را طوری پیکربندی کنید که به جای اجرای بعضی از کارها به طور دستی، آنها را به صورت خودکار و به عنوان عملیات توصیه‌شده انجام دهد. اگر گزینه‌های حفاظت پیوسته را بسیار زیاد می‌دانید، می‌توانید فهرست تنظیم‌های سیستم و فهرست رویدادهایی را که تحت نظر قرار می‌گیرند، اصلاح کنید. حتی می‌توانید این خصوصیت را غیرفعال کنید، اما ما این کار را توصیه نمی‌کنیم.

Microsoft SpyNet

تشخیص پایش‌افزار از برنامهٔ مجاز دشوار است. مایکروسافت از پایگاه SpyNet برای این منظور بهره می‌گیرد. پیوستن به SpyNet رایگان و اختیاری است. دو سطح از عضویت وجود دارد _ Basic و Advanced. آن را تحت Tools و Microsoft SpyNet می‌توانید بیابید.

یک مزیت پیوستن به SpyNet آن است که می‌توانید دریابید که کاربران دیگر Windows Defender، چگونه به یک برنامه پاسخ داده‌اند.

دفاع از خود

روزهایی که کاربران می‌توانستند برای حفاظت کامل از کامپیوتر خود صرفاً به یک برنامهٔ ضدویروس اتکا کنند گذشته است. اهمیت حفاظت ضدپایش‌افزاری روزبه‌روز افزایش می‌یابد، وWindows Defender یک روش خوب حفاظت از خودتان و کامپیوترتان در برابر نرم‌افزارهای ناخواسته است.□