چگونه از آنتی‌ویروس داخلی Windows Defender در ویندوز ۱۰ استفاده کنیم؟

ویندوز ۱۰ یک آنتی‌ویروس real-time به نام Windows Defender دارد که واقعا خیلی خوب است. این نرم‌افزار در پس‌زمینه ویندوز اجرا می‌شود و تمامی کاربران ویندوز را در مقابل ویروس‌ها و سایر عوامل مخرب محافظت می‌کند. در ادامه نگاهی بر چگونگی کارکرد Windows Defender داریم.

با به‌روز رسانیCreators ، رابط کاربری Windows Defender تا حدودی تغییر کرده و با مرکز ایمنی ویندوز یک‌پارچه شده است؛ مرکز ایمنی ویندوز، دسترسی به ابزارهای امنیتی مانند حفاظت از خانواده، تنظیمات فایروال، عملکرد دستگاه، گزارش‌های سلامتی و کنترل‌های امنیتی مرورگر را فراهم می‌کند. اگر هنوز به‌روزرسانی Creators را دریافت نکرده‌اید باز هم می‌توانید از این امکانات استفاده کنید.

Windows Defenderچیست؟

مایکروسافت به همراه ویندوزهایXP ، ویستا و ۷، یک برنامه آنتی‌ویروس مستقل به نام Microsoft Security Essentials را ارایه کرد؛ در ویندوز ۸ این محصول کمی با ویندوز ادغام شد و Windows Defender نام گرفت. این آنتی‌ویروس در مجموع عملکرد بسیار خوبی دارد؛ هرچند که مطابق بنچمارک‌ها سایر برنامه‌های آنتی ویروس مانند BitDefender و Kaspersky در برابر ویروس‌های بیشتری محافظت به عمل می‌آورند. با تمام این‌ها Windows Defender مزایای زیادی دارد. این برنامه بسیار غیرتهاجمی است؛ همه چیز را در پس‌زمینه کنترل و مدیریت می‌کند و مزاحمتی برای کاربر به وجود نمی‌آورد. همچنین در مرورگرهای وب و سایر برنامه‌های مرتبط با امنیت و حریم خصوصی عملکردی به مراتب بهتر از اکثر آنتی‌ویروس‌ها دارد.

هر آنتی ویروسی که استفاده می‌کنید به خودتان مربوط است اما Windows Defender انتخاب بدی نیست و در سالیان اخیر بیشتر مشکلات آن برطرف شده است. هرچند توصیه می کنیم در کنار آنتی‌ویروس خودتان یک برنامه ضد تروجان مانند Malwarebytes را هم نصب کنید.

از مزایایی مانند اسکن اتوماتیک و آپدیت‌های منظم برخوردار شوید.

مانند سایر آنتی‌ویروس‌ها، Windows Defender هم در پس‌زمینه اجرا می‌شود و فایل ها را در هنگام دانلود یا انتقال از درایوهای اکسترنال و قبل از اجرا اسکن می‌کند. لازم نیست هیچ‌وقت درباره عملکرد این نرم‌افزار فکر کنید؛ چون هنگام یافتن هرگونه بدافزاری فقط از طریق پاپ‌آپ شما را آگاه می‌کند و حتی نمی‌پرسد که با نرم‌افزارهای مخرب می‌خواهید چه کاری انجام دهید؛ فقط آن‌ها را پاک می‌کند و فایل‌ها را به‌صورت اتوماتیک قرنطینه می‌کند.

گاهی اوقات یک پنجره اطلاع‌رسانی را مشاهده خواهید کرد که به شما اطلاع می‌دهد یک اسکن انجام شده است؛ همچنین معمولا می‌توانید اطلاعات مربوط به آخرین اسکن را با باز کردن مرکز اقدام (Action Center) در ویندوز ۱۰ مشاهده کنید.

اگر Windows Defender یک تهدید پیدا کند، یک اعلان را خواهید دید که به شما اطلاع می‌دهد اقدامات لازم برای برطرف کردن تهدیدها انجام شده است و از شما هیچ کاری خواسته نمی‌شود.

به‌روزرسانی آنتی‌ویروس از طریق به‌روزرسانی ویندوز تعریف شده است و مانند سایر به روزرسانی‌های سیستمی نصب می‌شود. این نوع از به‌روزرسانی نیازی به راه اندازی مجدد کامپیوتر ندارد و به این ترتیب، لازم نیست در مورد آپدیت شدن Windows Defender نگران باشید؛ همه کارها به‌صورت بی سر و صدا و به‌طور خودکار در پس‌زمینه انجام می‌شود.

تاریخچه اسکن و بدافزارهای قرنطینه شده را ببینید

می‌توانید هرگاه که خواستید، تاریخچه اسکن Windows Defender را مشاهده کنید و اگر اعلانی درباره یک بدافزار مسدود شده دریافت کردید می‌توانید اطلاعات مربوط به آن را هم مشاهده نمایید. برای روشن کردن مرکز امنیت Windows Defender ، پس از باز کردن منوی Start ، کلمه "defender" را تایپ کنید و سپس "Windows Defender Security Center" را انتخاب کنید.

در پنجره Windows Defender Security Center ، به سربرگ "Windows Defender" (با نشانه سپر) بروید و روی لینک "Scan history" کلیک کنید.

صفحه "Scan history" تمام تهدیدات فعلی و همچنین اطلاعات مربوط به آخرین اسکن را به شما نشان می‌دهد. برای مشاهده سابقه کامل تهدیدهای قرنطینه شده، کافی است که روی لینک "See full history" کلیک کنید.

در این‌جا می‌توانید تمامی تهدیدهای قرنطینه شده توسط Windows Defender را مشاهده کنید. برای دیدن اطلاعات بیشتر درباره یک تهدید، روی فلش سمت راست آن کلیک کنید و اگر باز هم می‌خواهید بیشتر بدانید می‌توانید روی لینک "See details"کلیک کنید.

شما واقعا نیاز به انجام کار دیگری در این‌جا ندارید، اما اگر Windows Defender یکی از تهدیدهای یافت شده را حذف نکرده باشد می‌توانید در این صفحه این کار را انجام دهید. همچنین قادر به بازگرداندن آیتم‌ها از قرنطینه هستید اما فقط زمانی این کار را انجام دهید که اطمینان داشته باشید یک آیتم به اشتباه بدافزار تشخیص داده شده است. اگر کاملا اطمینان ندارید این کار را انجام ندهید.

انجام یک اسکن دستی

به صفحه اصلی Windows Defender بازگردید؛ در این‌جا می توانید با کلیک بر روی دکمه "Quick Scan" یک اسکن دستی انجام دهید. به‌صورت معمول، از آن‌جایی که این نرم‌افزار به‌صورت real-time کار می‌کند نیازی به اجرای اسکن دستی نیست و این کار به‌صورت منظم و اتوماتیک انجام می‌شود؛ با این حال به‌منظور حصول اطمینان، اجرای یک اسکن سریع ضرری ندارد.

شما همچنین می توانید روی لینک "Advanced scan" کلیک کنید تا سه نوع اسکن مختلف را اجرا کنید:

- **Full scan** : اسکن سریع فقط حافظه شما و مکان‌های رایج را اسکن می‌کند. یک اسکن کامل هر گونه فایل و برنامه اجرایی را بررسی می‌کند و به راحتی می‌تواند یک ساعت یا بیشتر طول بکشد، بنابراین بهتر است هنگامی این کار را انجام دهید که نیاز به استفاده از کامپیوترتان نداشته باشید.
- **Custom scan** : یک اسکن سفارشی به شما اجازه می‌دهد تا یک پوشه خاص را برای اسکن انتخاب کنید؛ می‌توانید این کار را با کلیک راست بر روی هر کدام از پوشه‌های کامپیوتر خود و انتخاب "Scan with Windows Defender"از منوی زمینه‌ای انجام دهید.
- **Windows Defender Offline scan** : زمانی که ویندوز در حال اجرا باشد حذف بعضی از نرم‌افزارهای مخرب آسان نیست. اگر اسکن آفلاین را انتخاب کنید سیستم ری‌استارت شده و قبل از لود شدن کامل ویندوز، اسکن کامل انجام می‌شود.
- تنظیمات پیکربندی محافظت در برابر ویروس‌ها و تهدیدهای امنیتی

در حالت پیش‌فرض، Windows Defenderبه‌صورت اتوماتیک محافظت real-time (بی‌وقفه)، محافظت بر پایه فضای ابری و ارایه نمونه‌ها را انجام می‌دهد؛ محافظت بی‌وقفه به شما اطمینان می‌دهد که این نرم‌افزار امنیتی به‌صورت اتوماتیک و همیشگی سیستم را اسکن کرده وبدافزارها را پیدا می‌کند می‌توانید در صورت لزوم، به منظور بالابردن کارایی سیستم در زمان کوتاهی این قابلیت را غیرفعال کنید، اما Windows Defender دوباره محافظت بی‌وقفه را فعال می‌کند تا تهدیدی متوجه سیستم نشود.

محافظت بر پایه فضای ابری و ارایه نمونه‌ها به Windows Defender امکان می‌دهد که اطلاعات خود را درباره فایل‌های مخرب و بدافزارها با مایکروسافت به اشتراک بگذارد.

برای فعال یا غیرفعال کردن هر یک از این تنظیمات، روی لینک "Virus & threat protection settings" در سربرگ اصلی Windows Defender کلیک کنید.

قرار دادن استثنا برای فولدرها یا فایل‌های خاص:

اگر در صفحه "Virus & threat protection settings" به قسمت پایین اسکرول کنید می‌توانید پوشه‌ها و فایل‌هایی را مشخص کنید که نمی‌خواهید Windows Defender آن‌ها را اسکن کند. برای این کار روی لینک "Add or remove exclusions" کلیک کنید.

اگر Windows Defender سرعت اجرای برنامه‌ای را که می‌دانید امن است، به دلیل اسکن کردن به مقدار قابل توجهی کاهش داده است، قرار دادن استثنا می‌تواند سرعت برنامه را به حالت قبل برگرداند. اگر از ماشین‌های مجازی استفاده می‌کنید ممکن است نخواهید این فایل‌های بزرگ را اسکن کنید و یا اگر مجموعه بزرگی از تصاویر و ویدیوها را دارید و می‌دانید که مشکلی ندارند احتمالا دوست ندارید که با اسکن کردن آن‌ها روند کلی اسکن را طولانی نمایید. برای قرار دادن استثنا، روی دکمه "Add an exclusion" کلیک کرده و سپس نوع استثنا را از منوی کشویی باز شده انتخاب کنید. حالا می‌توانید موارد دل‌خواه خود را از فرآیند اسکن کنار بگذارید.

فقط مراقب باشید که با دقت این کارها را انجام دهید؛ با هر استثنایی که تعیین کنید کمی از امنیت سیستم کاسته خواهد شد چون به این ترتیب به نرم‌افزار امنیتی ویندوز می‌گویید که برخی از موارد را بررسی نکند.

اگر یک آنتی‌ویروس دیگر نصب کنید چه اتفاقی می‌افتد؟

اگر یک آنتی‌ویروس دیگر نصب کنید ویندوز ۱۰ به‌صورت اتوماتیک Windows Defender را غیرفعال می‌کند؛ همچنین دیگر محافظت و اسکن real-time را به عمل نمی‌آورد تا با آنتی ویروس نصب شده تداخلی نداشته باشد. البته هنوز هم می‌توانید این نرم‌افزار را به‌صورت دستی یا آفلاین اجرا نموده و به‌عنوان پشتیبان آنتی‌ویروس اصلی داشته باشید.

اگر آنتی‌ویروس نصب شده را حذف کنید Windows Defender دوباره فعال می‌شود تا از سیستم محافظت کند.

در ضمن توجه داشته باشید که نرم‌افزارهای ضدتروجان مانند Malwarebytes می‌توانند در کنار نرم‌افزار امنیتی پیش‌فرض ویندوز نصب شده و با هم محافظت real-time را انجام دهند.

هر آنتی‌ویروسی را که گمان می‌کنید خوب است نصب کنید اما بدانید که ویندوز ۱۰ به همراه یک آنتی‌ویروس پیش‌فرض ارایه شده است. شاید گمان کنید که این نرم‌افزار به اندازه کافی خوب نیست اما کمترین مزاحمت را به همراه دارد و هنگامی که با رعایت سایر اصول امنیتی استفاده از کامپیوتر و مرور اینترنت همراه شود ممکن است به‌تنهایی برای محافظت از سیستم شما کافی باشد.