**آنتی ویروس چیست؟**

**آنتی ویروس چیست و چگونه عمل می‌کند؟**

آنتی ویروس چیست؟ احتمالاً از زمانی که کامپیوتر داشتید در مورد نرم افزار آنتی ویروس شنیده اید. از اوایل دهه 90 اگر از هر یک از کارکنان IT مورد اعتماد در مورد نحوه محافظت از سیستم خود در برابر هکرها و تهدیدها بپرسید، آن‌ها همان پاسخ را به شما می دهند: یک راه حل ضد ویروس نصب کنید.

اگر از بهترین روش‌ها برای ایمن ماندن در اینترنت استفاده می‌کنید، مانند نادیده گرفتن لینک‌ها و پیوست‌ها در ایمیل‌های غیرقابل اعتماد، اجتناب از وب سایت‌های مبهم و پایبند بودن به فروشگاه‌های برنامه‌های تحت نظارت ممکن است کامپیوتر شما کار کند، اما همچنان خطر در کمین است.

اما نرم افزار آنتی ویروس چیست و چگونه کار می‌کند؟ تعاریف متعددی وجود دارد و بسته به محصول شرکتی که استفاده می‌کنید، تاکتیک‌های آن‌ها برای هدف قرار دادن برنامه‌های مخرب مانند ویروس‌ها و باج افزارها می‌تواند کاملاً متفاوت باشد. آگاهی کامل از آنچه این نوع ابزارها می‌توانند انجام دهند بهترین راه برای انتخاب آگاهانه در مورد بهترین نرم افزار آنتی ویروس برای شما یا مشاغل کوچک شما است.

آنتی ویروس چیست؟ آنتی ویروس به نرم افزاری گفته می‌شود که مسئولیت پاکسازی و جلوگیری از ورود ویروس و عوامل مخرب به کامپیوتر را بر عهده دارد. در واقع آنتی ویروس یک برنامه کامپیوتری است که برای مرور فایل‌ها و تشخیص و حذف ویروس‌ها و دیگر بدافزارها از آن استفاده می‌شود. نرم افزار آنتی ویروس‌، گاهی اوقات به عنوان نرم افزار ضد بدافزار شناخته می شود، برای تشخیص، جلوگیری و اقدام برای خلع سلاح یا حذف نرم افزارهای مخرب از رایانه شما مانند ویروس ها، کرم ها و اسب های تروا طراحی شده است. همچنین ممکن است علاوه بر انواع دیگر برنامه های مخرب، از جاسوس افزارها و ابزارهای تبلیغاتی مزاحم ناخواسته جلوگیری یا حذف کند. اولین نسخه های نرم افزار آنتی ویروس را می توان در دهه 1990 جستجو کرد.

**نحوه عملکرد آنتی ویروس‌ها**

هسته مرکزی یک آنتی ویروس، موتور جستجوی آن است. این موتور از الگوریتم‌های جستجو برای بررسی لایه‌های مختلف فایل‌ استفاده می‌کند.

موتور جستجو با الگوریتم مخصوص به خود میلیون‌ها فایل را در مدت زمان کوتاهی بررسی می‌کند و از شناسه‌ها برای ردیابی فایل‌های آلوده و مخرب استفاده می‌کند. شناسه، بخشی از رشته لایه‌های مختلف فایل‌ها را در بر دارد و مانند اثر انگشت برای هر ویروس یکتا است.

یکی از مزیت‌های استفاده از آنتی ویروس‌های معتبر و خرید لایسنس قانونی آن‌ها، این است که شرکت سازنده خود را موظف می داند تا از طریق به روزرسانی بانک شناسه‌ها، شما را در مقابل جدیدترین ویروس‌ها محافظت نماید.

یکی دیگر از قابلیت‌هایی که بیشتر برنامه‌های آنتی ویروس در موتور جستجوی خود ایجاد می‌کنند، توانایی شناسایی رفتارهای مشکوک فایل‌ها و ایجاد سطوح دسترسی برای برنامه‌های مختلف است.

به این ترتیب حتی اگر شناسه ویروسی در بانک اطلاعاتی آنتی ویروس موجود نبود، موتور جستجو به طور خودکار رفتار فایل‌ها را زیر نظر می گیرد و اگر رفتار مشکوکی مشاهده کند به کاربر اخطار می‌دهد.

این روزها اکثریت شرکت‌های سازنده آنتی ویروس، برای جامع‌تر ساختن راه حل‌های امنیتی، قابلیت‌های [Firewall](https://softyab.com/what-is-firewall/)، آنتی [اسپم](https://softyab.com/4557-2/)و آنتی [فیشینگ](https://softyab.com/%d8%a2%d8%b2%d9%85%d9%88%d9%86-%d9%81%db%8c%d8%b4%db%8c%d9%86%da%af-%d8%a8%d8%b1%d8%a7%db%8c-%da%a9%d8%a7%d8%b1%da%a9%d9%86%d8%a7%d9%86-%d8%b3%d8%a7%d8%b2%d9%85%d8%a7%d9%86-%d9%87%d8%a7/) را نیز به نرم افزارهای خود اضافه می‌نمایند.

رفتار آنتی ویروس چیست؟ رفتار آنتی ویروس با ویروس معمولا توسط کاربر تعیین می‌شود. پیش فرض بیشتر آنتی‌ ویروس‌ها خنثی سازی فایل آلوده با از بین بردن کد مخرب است. در حالتی که کد قابل جداسازی نباشد آنتی ویروس آن را پاک و یا قرنطینه می‌کند.

در ادامه با برخی از تکنیک‌های رایج که در بین آنتی ویروس‌ها، برای تشخیص بدافزارها به کار برده می‌شوند، به طور دقیق تر آشنا خواهیم شد.

**تشخیص بر اساس شناسه ویروس**

اغلب برنامه‌های آنتی ویروس در حال حاضر از این تکنیک استفاده می‌کنند. در این شیوه، درایوهای حافظه و فایل ها، با هدف پیدا کردن الگویی که نشان دهنده یک بدافزار باشد، مورد جستجو قرار می‌گیرند.

این الگوها معمولا در فایل‌هایی به نام فایل های امضا ذخیره می‌شوند. فایل‌های مذکور توسط تولیدکنندگان نرم افزارهای آنتی ویروس طبق یک برنامه منظم به روز رسانی می‌شوند تا قادر باشند بیشترین تعداد ممکن حمله‌های بدافزاری را شناسایی کنند.

در این شیوه زمانی که نرم افزار آنتی ویروس یک فایل را مورد آزمایش قرار می‌دهد، به یک دیکشنری ویروس که حاوی امضای ویروس‌های شناخته شده است مراجعه می‌کند. در صورتی که هر تکه از کد فایل با یک ویروس شناخته شده مطابقت داشته باشد، فایل مذکور به عنوان یک فایل آلوده شناسایی شده و آنتی ویروس یا آن را پاک می‌کند و یا آن را قرنطینه می‌نماید تا برنامه‌های دیگر به آن دسترسی نداشته و همچنین از انتشار آن جلوگیری به عمل آید. در برخی موارد نیز امکان بازسازی فایل آلوده از طریق حذف ویروس از فایل اصلی وجود دارد که در صورت امکان آنتی ویروس این کار را انجام می‌دهد.

مشکل اصلی تکنیک بررسی شناسه این است، که آنتی ویروس نسبت به ویروس‌های جدید آسیب پذیری بسیار بالایی دارد و تقریبا خنثی عمل خواهد کرد. چون در این روش، بانک اطلاعاتی آنتی ویروس باید قبلا به روز رسانی شده باشد تا بتواند به مقابله و خنثی سازی بدافزارها بپردازد و لذا بدافزارهای جدیدی که هنوز شناسایی نشده و به فایل‌های امضا، اضافه نشده‌اند تشخیص داده نمی‌شوند.

مسئله دیگری که باید به آن توجه کرد، این است که ویروس نویسان همواره تلاش می‌کنند تا یک قدم جلوتر از آنتی ویروس‌ها حرکت کنند و این کار را از طریق ایجاد ویروس‌های چندریختی انجام می‌دهند. ویروس های چندریختی در واقع دارای یک مکانیزم دفاعی رمزنگاری هستند.

روشهای متنوعی برای رمزنگاری و بسته بندی بدافزارها وجود دارد که تشخیص انواع شناخته شده بدافزارها را برای آنتی ویروس‌ها بسیار سخت می‌سازد. متاسفانه بسیاری از آنتی ویروس‌های معروف امروزی فاقد توانایی تشخیص ویروس‌های رمزنگاری شده هستند.

**تشخیص رفتاری ویروس**

در این روش بر خلاف روش پیشین، آنتی ویروس تنها در تلاش برای شناسایی ویروس‌های شناخته شده نیست بلکه رفتار همه برنامه‌ها را نظارت می‌کند. این تکنیک سعی در تشخیص انواع شناخته شده و همچنین انواع جدید بدافزار دارد و این کار را از طریق جستجوی ویژگی‌های عمومی و مشترک [بدافزارها](https://softyab.com/%d8%aa%d8%b9%d8%b1%db%8c%d9%81-%d9%88%db%8c%d8%b1%d9%88%d8%b3-%db%8c%d8%a7%d8%a8-%d8%a7%d8%b2-%d8%b2%d8%a8%d8%a7%d9%86-g-data/) انجام می‌دهد.

به عنوان مثال اگر یک برنامه سعی در نوشتن داده بر روی یک برنامه اجرایی دیگر را داشته باشد، این رفتار به عنوان یک رفتار مشکوک شناسایی شده و به کاربر هشدار لازم داده می‌شود. سپس از او در مورد اینکه چه کاری باید انجام شود سوال می‌شود.

به روش تشخیص بر اساس رفتار، جستجوی اکتشافی یا Heuristic نیز گفته می‌شود زیرا سعی در کشف رفتارهای مشکوک و شناسایی بدافزارها دارد. مهمترین فایده این روش تکیه نکردن آن بر فایل‌های امضا برای تشخیص و مقابله با بدافزار است.

البته این روش نیز با مشکلات خاصی روبرو است از جمله کندتر بودن این روش نسبت به روش تشخیص بر اساس امضا و تعداد زیاد تشخیص‌های مثبت اشتباه و هشدارهای بی مورد به کاربر، که موجب خستگی و سر رفتن حوصله کاربران می‌شود.

همچنین در این روش نیز در صورتی که یک حمله بدافزاری جدید، ویژگی‌هایی را از خود به نمایش بگذارد که پیش از این شناسایی نشده‌اند، جستجوی اکتشافی نیز آن را شناسایی نمی‌کند مگر اینکه به روز رسانی شده و ویژگی مذکور به حافظه آن اضافه شود.

**استفاده از Sandbox**

یکی دیگر از روش‌های تشخیص ویروس، استفاده از sandbox است. یک sandbox سیستم عامل را شبیه سازی کرده و فایل‌های اجرایی را در آن اجرا می‌کند. بعد از پایان اجرای برنامه‌ها، sandbox در مورد تغییراتی که ممکن است نشان دهنده ویروس باشد مورد ارزیابی قرار می‌گیرد. به علت سرعت پایین این روش تشخیص، از آن فقط در صورت تقاضای کاربر استفاده می‌شود.

**استفاده از فناوری Cloud**

در نرم افزارهای آنتی ویروس رایج و امروزی، یک فایل یا برنامه جدید، تنها توسط یک تشخیص دهنده ویروس در یک زمان مورد بررسی قرار می‌گیرد. اما آنتی ویروس ابری می‌تواند برنامه‌ها یا فایل ها را به یک شبکه ابری ارسال کند که در آن از چندین آنتی ویروس و چندین ابزار تشخیص بدافزار به صورت همزمان استفاده می‌شود.

آنتی ویروس ابری در واقع یک آنتی ویروس مبتنی بر محاسبات ابری است که توسط دانشمندان دانشگاه میشیگان تولید شده است. هر زمان که رایانه یک فایل یا برنامه جدید را دریافت یا نصب کند، یک نسخه از آن به صورت خودکار برای ابر آنتی ویروس ارسال می‌شود و در آنجا با استفاده از ۱۲ تشخیص دهنده متفاوت که با یکدیگر کار می‌کنند، مشخص می‌شود که آیا باز کردن فایل یا برنامه مذکور امن است یا خیر.

همان طور که خواندید، هر کدام از روش‌های فوق دارای مزایا و معایبی می‌باشد و هیچ یک به تنهایی نمی‌تواند روشی کامل و ایمن به حساب آید. بنابراین اکثریت آنتی ویروس‌های معتبر، محبوب و قدرتمند سعی می‌کنند از مجموعه و ترکیبی از روش‌های فوق برای شناسایی و پاکسازی ویروس‌ها و فایل‌های مخرب استفاده نمایند تا میزان  اثرگذاری خود را افزایش دهند.

منبع: [digitaltrends](https://www.digitaltrends.com/computing/what-is-antivirus-software/)، [geeksonsite](https://www.geeksonsite.com/computer-security/what-does-virus-scan-do-how-antivirus-software-works/)

لطفا جهت مشاوره در [انتخاب آنتی ویروس مناسب](https://softyab.com/product-category/security/antivirus/) خود با این شماره **09224971053** تماس بگیرید.

**مارو در شبکه های**[اجتماعی](https://www.instagram.com/softyab)**خودتان به اشتراک بگذارید.**