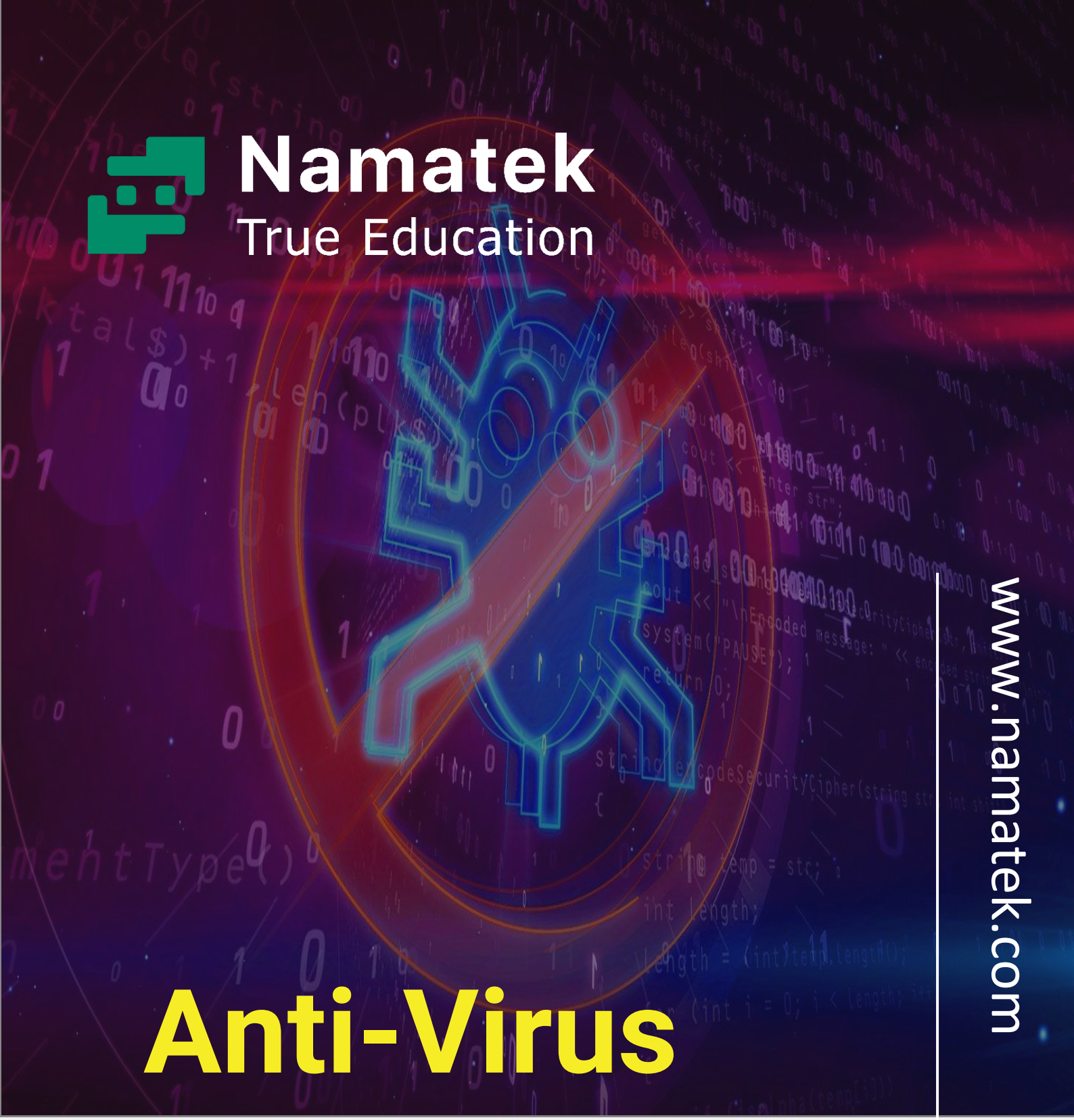
Namatek
True Education



Anti-Virus

www.namatek.com

آنتی ویروس چیست؟ (۳ روش برای اسکن سیستم)

فهرست مطالب

حملات ویروسی به سیستم های کامپیوتری و سرقت اطلاعات شخصی همواره یکی از ترس های کاربران این سیستم هاست که با توجه به داشتن آگاهی درباره اینکه آنتی ویروس چیست و چطور کار می کند می توان از این نگرانی ها کاست. از آنتی ویروس برای شناسایی، اسکن و حذف ویروس های مخرب استفاده می شود و از این طریق از فایل ها و اطلاعات موجود در سیستم کامپیوتری محافظت به عمل می آید.

برای کسب اطلاعات بیشتر در خصوص آنتی ویروس و کاربرد آن، با ما همراه باشید.

#۱ آنتی ویروس چیست؟ (Anti-Virus Software)

نرم افزار های آنتی ویروس برای ارزیابی اطلاعاتی مانند فایل ها، صفحات وب و نرم افزار ها طراحی و اجرا می شوند و با یافتن و ریشه کن کردن بدافزارها در کوتاه ترین زمان ممکن، از نفوذ ویروس جلوگیری می کنند. از آن جایی که بیشتر فعالیت های رایانه ای به صورت آنلاین انجام می شوند، تهدیدهای ویروسی برای اکثر سیستم ها وجود دارند. نصب یک برنامه آنتی ویروس روی سیستم بهترین و سریع ترین راهکار برای مواجهه با این تهدیدها است. سیستم باید در برابر ورود ویروس و سایر آسیب

های بدافزارها اسکن و به روز رسانی شود. با نصب آنتی ویروس، کدها و سایر برنامه های مخرب شناسایی شده و درنهایت حذف می شوند.

آنتی ویروس ها سه وظیفه اصلی بر عهده دارند که عبارت اند از:

۱. بازرسی و کشف ویروس
۲. شناسایی هویت ویروس
۳. حذف و پاکسازی کامل سیستم از انواع ویروس

سیستم هایی که آنتی ویروس ندارند یا آنتی ویروس نصب شده در آن ها به روز رسانی نشده است، به شدت در معرض حمله ویروس ها و بدافزارها قرار خواهند گرفت. از همین رو، تاکید می شود حتما نسبت به نصب نرم افزار آنتی ویروس جدید اقدام شود. امروزه تعداد زیادی نرم افزار آنتی ویروس کاربردی در سایت های رسمی و معتبر در دسترس هستند که هر کاربر می تواند متناسب با ویژگی های سیستم خود آن ها را تهیه کند.

حال این سوال مطرح می شود که ویژگی های شاخص آنتی ویروس چیست که این نرم افزار را جزء ضروریات یک سیستم قرار می دهد؟

#۲ مهم ترین ویژگی های آنتی ویروس چیست؟

به نظر شما موارد قابل بررسی در انتخاب یک آنتی ویروس قوی چیست؟ برخی از مهم ترین ویژگی های انواع آنتی ویروس عبارت اند از:

- برخورداری از پایگاه داده قوی و منسجم
- قابلیت آپدیت شدن
- امکان اسکن و شناسایی انواع بدافزارها مانند تروجان (Trojan)، ورم ها(Worms) و ویروس های مخرب (Malicious Viruses)
- عدم ایجاد تاخیر در اجرای برنامه های مختلف
- قابلیت اسکن سیستم در زمان بوت (Boot) شدن (بوت شدن سیستم به معنی روشن و آماده به کار شدن رایانه است)
- توانایی بالا برای حذف و پاک سازی کامل ویروس ها و بدافزارها
- پشتیبانی مداوم از سیستم
- قابلیت ذخیره سازی فایل های به روز رسانی شده برای استفاده در آینده
- برخورداری از سرعت بالا برای اسکن سریع سیستم
- کاربری آسان و اجرای خودکار

#۳ آشنایی با انواع ویروس سیستمی

ویروس های کامپیوتری برنامه های مخربی هستند که از راه های زیر وارد سیستم می شوند:

- وب سایت های آلوده
- ایمیل ها
- کلیک روی فایل های اجرایی
- استفاده از حافظه های قابل حمل و نرم افزار های تقلبی

برخی از انواع ویروس های مخرب عبارت اند از:

- ساکن (Resident)
- عمل مستقیم (Direct Action Virus)

- بوت سکتور (Boot Sector Virus)
- چندریختی (Polymorphic)
- چند مرتبه ای (Overwrite Virus)
- برنامه (Program)
- مخفی (Stealth)
- زره پوش (Armored)
- رمزنگاری (Encrypted)

#۴ نحوه عملکرد آنتی ویروس

آنتی ویروس ها در بَدو ورود به سیستم تمام فایل های اجرایی را اسکن می کنند. آن ها یک پایگاه داده اختصاصی دارند؛ بنابراین تمام فایل ها و اطلاعات داخل سیستم را با پایگاه داده خود مقایسه می کنند. آنتی ویروس ها در صورت شناسایی فایل های مشکوک به ویروس یا مخرب، این دسته از فایل ها را به لیست سیاه (Black List) ارسال می کنند. در نهایت آنتی ویروس فایل های مشکوک ارسال شده را چک می کند و در صورت لزوم آن ها را برای بازبینی و شناسایی دقیق تر به بخش لابراتور اختصاصی ارسال می کند

(کمپانی های سازنده آنتی ویروس، لابراتوری دارند که با جدیدترین فناوری های روز دنیا همراه است. کاربران با ورود به سایت آنتی ویروس، به لابراتور اختصاصی متصل می شوند. سایت مورد نظر فایل ها و اطلاعات مخرب کاربران را دریافت نموده و پس از اسکن آن ها، ویروس ها را شناسایی و آن ها را حذف می کند.)

پس از اسکن و شناسایی کامل ویروس ها، فایل های سالم وارد فاز اجرایی می شوند. از سوی دیگر، فایل هایی وجود دارند که ناشناخته هستند و برای آن که سالم یا معیوب بودن آن ها مشخص شود، به سیستم دفاعی آنتی ویروس و جعبه شنی (فضایی در آنتی ویروس برای ذخیره و تست فایل های مشکوک) ارسال می شوند. تمام اطلاعات ارسال شده به جعبه شنی (Sandbox) برای بررسی دقیق تر به سایر سرورهای

شرکت سازنده آنتی ویروس ارسال می شوند و پس از بازبینی و بررسی کامل، درنهایت پاک سازی کامل سیستم از ویروس های مخرب انجام می شود.

#۵ انواع روش های اسکن سیستم

نرم افزار های آنتی ویروس به سه روش اقدام به اسکن سیستم ها می کنند. در این بخش از مقاله روش های مختلف اسکن سیستم را بیان می کنیم.

#۵-۱ منظور از اسکن کامل در آنتی ویروس چیست؟ (Full Scan)

در این شیوه کل سیستم از جمله موارد زیر، توسط آنتی ویروس مورد بررسی قرار می گیرد.

- حافظه های قابل حمل
- تمام هارد دیسک ها و درایورهای شبکه
- فایل های پشتیبانی
- حافظه موقت
- واحدهای رجیستری

...9

با توجه به میزان داده ذخیره شده در سیستم، زمان اسکن متغیر است. تمام داده ها به صورت کامل تجزیه و تحلیل می شوند. دوره زمانی این نوع اسکن دو مرتبه در ماه، توسط آنتی ویروس آپدیت شده است.

#۲-۵ منظور از اسکن هوشمند یا سریع در آنتی ویروس چیست؟ (Smart or Fast Scan)

برخی از نرم افزار های آنتی ویروس جدید توانایی اسکن سریع را دارند و موارد زیر را مورد بررسی قرار می دهند:

- حافظه موقت سیستم
- انواع فایل ها و پوشه های آلوده

- تمام فایل های استارتاپ
- واحدهای رجیستری

و...

شاید عملکرد اسکن سریع با عملکرد اسکن کامل مشابه به نظر برسد؛ اما تفاوت این جاست که در اسکن سریع و هوشمند، به جای آن که تک تک برنامه ها و فایل ها اسکن شوند، تنها مکان هایی مورد بررسی قرار می گیرند که احتمال فعالیت ویروس و بدافزارها در آن جا زیاد باشد. بدین ترتیب، مراحل و زمان انجام عملیات اسکن سریع در مقایسه با اسکن کامل کاهش می یابد. از سوی دیگر، برخی از نرم افزار های آنتی ویروس تنها فایل هایی را اسکن سریع می کنند که در آخرین عملیات اسکن روی آن ها اصلاحات انجام شده است. در این شیوه آنتی ویروس به طور مداوم در حال بررسی و یافتن اطلاعات جدید است تا به کاربر اطلاع رسانی کند. دوره زمانی عملیات اسکن سریع حداقل هفته ای دو تا سه بار است.

#۳-۵ منظور از اسکن سفارشی در آنتی ویروس چیست؟ (Custom Scan)

همان طور که از نام این نوع اسکن مشخص است، امکان انتخاب فایل های مورد نظر برای اسکن وجود دارد. این شیوه نیز مانند اسکن کامل به طور دقیق و جامع به بررسی تمام فایل های انتخاب شده می پردازد. به عنوان مثال می توان عملیات اسکن را روی درایو C که محل ذخیره سازی و اجرای برنامه های مهم سیستم است، انجام داد. مدت زمان این شیوه نسبت به روش اسکن کامل، کمتر است.