چطور یک آنتی ویروس رایگان (Free) می تواند هزینه ها و انرژی شما را هدر دهد

ترجمه: مهندس مصطفی شمیزی

خلاصه:

نرم افزارهای آنتی ویروس رایگان ممکن است خیلی مقرون به صرفه بنظر برسند، اما این نرم افزاره،ا نکات و موارد ضروری را که می بایست قبل از دانلود کردن و نصب آنها بدانید را در اختیار شما قرار نمی دهند.

در نوعی نگاه اقتصادی، بدست آوردن هر آنچه رایگان در اختیار شما قرار گیرد چیز خوبی است. آیا این نوع نگرش صحیح است؟ کوتاه ترین پاسخ این است: بستگی به میزان ریسکی که قبول می کنید، دارد.

استفاده از آنتی ویروس های رایگان می تواند مثال خوبی به این پاسخ باشد. انتخاب آنتی ویروس رایگان می توان در ظاهر مقرون به صرفه باشد، اما در اصل چنین نیست. در اینجا به نکاتی که می بایست قبل از دانلود هر نرم افزار رایگانی به آنها توجه داشته باشید اشاره می کنیم.

نخستین و اصلی ترین مورد این است که تهیه کنندگان آنتی ویروس های رایگان تمام آنچه که در برابر نفوذ و تهدیدهای بزرگ شبکه ای بروزی که مورد نیازتان است را در اختیارتان قرار نمی دهند. بنابر این موقعی که شما کامپیوتر، نرم افزارها و سایر فایلها و اطلاعات شخصی خود را به اطمینان آنتی ویروس رایگان در شبکه و اینترنت بکار میگیرید، در واقع وقت شما را به هدر دهد و بدتر از آن پولی را که تصور میکردید صرفه جویی کردید.

اغلب آنتی ویروس های رایگان در واقع طعمه هایی هستند که برای استفاده از نرم افزارهای اصلی برای شما دام می گسترند. آنها معمولا یک نسخه ای از نرم افزار پولی خود را که فقط تعداد محدودی از تهدیدها و ویروس های بزرگ اینترنتی را شامل می شوند و بسیار کم حجم می باشد را در اختیار شما قرار می دهند.

پس از اینکه شما آنتی ویروس رایگان را نصب کردید، انتظار دارید که سد برگی در برابر ویروسها و تروجانهای آزار دهنده ایجاد کرده باشید، در حالیکه منویی در دستکاپ ظاهر می گردد و پیامی مبنی بر اینکه آنتی ویروس رایگان نصب شده تنها مانع از حمله ویروس و تروجان شده و برای حذف آن می بایست نسخه پولی آن را تهیه کنید را اعلام می کند. و یا پیامهای مشابه مثال فوق را برای ایمن سازی کامپیوترتان به شما میدهند. و تقاضای پرداخت پول برای رفع مشکل می نمایند.

یک راه عبور آزاد برای آخرین تهدیدها

نکته دیگری که می بایست به خاطر داشته باشید اینکه: اغلب متخصصین امر معتقدند بزرگترین تهدیدهای بروز اینترنتی و شبکه ای به گونه ای وارد سیستم می شوند که نرم افزارهای ضد ویروس رایگان نمی توانند مانع از ورود آنها باشند. Rootkit, bots, key loggers, hackers, phishing scams, و وب سایت های آلوده به آسانی از سد آنتی ویروس های رایگان عبور کرده اند.

این تهدیدها حتی میتوانند بسیار گسترده تر و خطرناک تر از ویروسها باشند، نه تنها کامپیوتر و فایلهای شخصی موجود در آن، بلکه حساب های بانکی شما را نیز تهدید کنند. آنها می توانند باعث آسیب اطلاعات هارد دیسک و خرابی سیستم شده، و بدتر از همه اطلاعات شخصی شما را بدزدند. و استفاده از آنتی ویروس رایگان برای شما بسیار گران تمام شود.

همچنین، آنتی ویروس های رایگان معمولا واکنش گرا است. بدین معنی که آنتی ویروس های رایگان موقعی وارد عمل میشوند که مورد حمله واقع می شوند و درست موقعی عمل می کنند که کامپیوتر و فایلهای موجود بر روی آن آسیب دیده اند.

و این تمام ماجرا نیست. زیرا نرم افزارهای ضد ویروس رایگان، برای جلوگیری از عملکرد تهدیدها به شما پیشنهاد جستجو، داونلود، تنظیم و نصب یک فایر وال و ضداسپم خاصی را که واقعا مورد نیازتان است، می دهند.

اینها زمان بر می باشند. اما هدر رفتن زمان شما به اینجا ختم نمی شود. موقعی که شما تنظیمات مربوط برای ایجاد امنیت برای جلوگیری از نفوذ یک تهدید خاصی را انجام می دهید، ممکن است باعث ایجاد تداخل در عملکرد سایر نرم افازهای سیستم و ایجاد پیامهای خطا و حتی آسیب درایوها شوید. حتی زمان بیشتری نیز صرف بازیابی و اصلاح موارد آسیب دیده خواهید کرد.

با این اوصاف نظرتان در باره این جمله چیست؟ آنتی ویروسهای رایگان نرم افزارهای مناسبی برای جلوگیری از تهدیدهای روزمره ای که کامپیوتر شما را مورد هدف قرار می دهند نیستند. هنگامی که به لیست قیمت نرم افزارها نگاه میکنید، متوجه باشید که **آنتی ویروسهای مجانی در واقع مجانی نیستند.**

منبع:

http://www.symantec.com/business/resources/articles/article.jsp?aid=20110720_free_antivirus_software