روش‌های مدیریت آنلاین هویت (اطلاعات شخصی)

حمید وثیق‌زاده انصاری

باظهور وبسایت‌های اجتماعی، دنیاواقعا کوچک شده است. با فشردن یک دکمه می‌توانیم اطلاعاتی مثل تاریخچه زندگی یک فرد، علایق و چیزهایی که مورد علاقه‌اش نیست و مدارک تحصیلی و مانند آن را در اختیار داشته باشیم، بنابراین چه روش‌هایی به ما کمک می‌کنند تا پروفایل خوب و مناسبی درباره خود برای کارفرمایان آماده کنیم؟ ادامه متن را بخوانید تا به فهم دقیقی از این موضوع دست پیدا کنید.

«اولین تاثیر، بهترین (آخرین) تاثیر است». این ضرب‌المثل را به‌طور حتم از کودکی تاکنون بارها شنیده‌اید. این یک ضرب‌المثل مذهبی است که از طرف مدیران، شرکت‌ها و البته دوستانتان رعایت می‌شود. داشتن اطلاعات شخصی (هویت) آنلاین مانند این است که شما در یک خانه با درهای شیشه‌ای زندگی می‌کنید و تمام فعالیت‌های زندگی شما برای دیگران مانند یک کتاب باز است. داشتن مشخصات آنلاین به‌طور قطع برای شما مفید است و به شما کمک می‌کند تا با دیگران ارتباط برقرار کنید. برای مثال به شرکت‌ها کمک می‌کند تا با مشتریان و تهیه‌کنندگان خود ارتباط برقرار کنند و همچنین به شرکت‌ها کمک می‌کند تا به اطلاعات مهمی درباره رقیبان خود دست پیدا کنند. در واقع این وبسایت‌های اجتماعی دنیایی کاملا جدید را خلق کرده‌اند اما این وبسایت‌های اجتماعی مزایا و معایب خاص خود را دارند. همیشه ترس از هکرهایی که می‌توانند به پروفایل (اطلاعات شخصی) شما نفوذ و تغییراتی را در آن ایجاد کنند یا از راه‌های غیر قانونی اطلاعات شما را بدزدند، وجود دارد. خطر هکرها حتی برای شرکت‌ها نیز مطرح است، چراکه هکرها می‌توانند به‌راحتی به اطلاعات حیاتی شرکت‌ها مثل اسرار تجاری یا اطلاعات مالی، دست یابند.

مدیریت آینده شما

یک نام تجاری شخصی می‌تواند برای شما هویت خوبی بسازد یا آن را خراب کند، شما باید به‌صورت مرتب به پروفایل شخصی خود سر زده و برای جلوگیری از پیش آمدن مشکلی که باعث خجالت شما شود، آن را کنترل کنید، این یک امر حیاتی است. در زیر برخی از روش‌هایی که می‌تواند در مدیریت مشخصات آنلاین (پروفایل) شما سودمند باشد، آمده است:

درباره هویت (چگونگی ساخت یک پروفایل مناسب برای خود) جست‌وجو کنید

بعد از این که پروفایل خود را ایجاد کردید، لازم است برای این که در مورد خودتان بیشتر (به‌منظور ویرایش پروفایل متناسب با خود) بدانید از موتورهای جست‌وجوی مختلف استفاده کنید. این کار به شما ایده‌هایی برای بیان کردن توانایی‌هایتان ارائه می‌دهد و مانند یک تذکر دهنده، برای جلوگیری از تبلیغات منفی به‌وسیله خودتان عمل می‌کند. به گفته یک مجله کسب و کار، حدود ۷۰ درصد استخدام‌ها با جست‌وجو در اطلاعات شخص متقاضی انجام می‌شود و ۳۰ درصدی که در آن متقاضی رد می‌شود، به‌دلیل یافت شدن برخی موارد نامناسب در اطلاعات شخصی متقاضی است. بسیاری از موتورهای جست‌وجو به شما خدمات شخصی مثل هشدار دادن را در صورتی که در مشخصات شما مورد نامناسبی یافت شود، ارائه می‌دهند. کنترل پروفایل خصوصی خود را با فعال کردن تنظیمات حریم خصوصی برای عکس‌ها، لیست دوستان و پیام‌ها، بر عهده بگیرید. یک روش حرفه‌ای‌تر استفاده از سایت‌های حرفه‌ای مانند لینکداین است که شانس دیده شدن شما را در استخدامی‌ها بالا می‌برد.

نکات منفی را پاک کنید

دهان به دهان گشتن در دنیای تبلیغات بسیار مهم است، برای مثال مطالب نوشته شده در مورد شما در وبلاگ دوستانتان و وبسایت‌های اجتماعی مانند یک زنگ خطر عمل می‌کنند که نباید آنها را نادیده بگیرید. اگر مطالب یا عکس‌های بی‌ربط خاصی در مورد خود پیدا کردید، سعی کنید حذفشان کنید یا به دوستان خود بگویید آنها را حذف کنند. همچنین توصیه می‌شود که خود را از خرده‌فعالیت‌های جنایی که باعث بدنام شدن تصویر و شخص شما می‌شوند، دور نگاه دارید.

مشکلات مربوط به گفتار

در حالی که شما مشغول چت کردن با یک نفر در نقطه دیگری از دنیا هستید، به‌طور قطع کسی در حال بررسی پروفایل و نظرات شما است. پس حواستان به گفتارتان باشد. سعی کنید که به‌عنوان یک فرد متعصب نسبت به مسائل خاص دیده نشوید. درست مانند بعد از یازده سپتامبر که بسیاری از مردم پیام‌هایی با محتوای نفرت را روی پروفایل خود نوشتند که این کار بی‌شک به‌نفع آنها نبود. همچنین خود را در گیر شایعه‌پراکنی‌ها (سوءظن) نکنید. همیشه به خود یادآوری کنید که اینترنت مانند پنجره‌ای است که از طریق آن هر کسی می‌تواند دنیای شما را زیر چشمی نگاه کند.

اطلاعات دقیقی را روی پروفایل خود قرار دهید

همان‌طور که به ما گفته می‌شود در پاسخ دادن به سوالات امتحانی جواب دقیق سوال را بنویسیم، همین روش از سوی سایت‌های حرفه‌ای نیز دنبال می‌شود. وقتی که یک کارفرما در حال جست‌وجوی مشخصات شما است، می‌خواهد اطلاعات دقیقی از شما و دستاوردهایی را که به‌تازگی کسب کرده‌اید ببیند، نه اطلاعاتی که قدیمی شده‌اند و دیگر به کار نمی‌آیند، پس همیشه پروفایل خود را به‌روزرسانی کنید و سعی کنید اطلاعاتی را که با کار شما مرتبط هستند و باعث تقویت رزومه شما می‌شوند، ارائه دهید.

پروفایل‌های (حساب کاربری‌های) اضافی را ببندید

پس از یک دوره زمانی، همه ما تمایل پیدا می‌کنیم که چندین حساب کاربری را در شبکه‌های اجتماعی مختلف ایجاد کنیم که بعدا به حالت غیر فعال و دروغین در می‌آیند. این حساب‌ها از طریق هکرها برای سرقت اطلاعات با ارزش شما مورد هدف قرار می‌گیرند که می‌توانند شما را در شرایط سختی قرار دهند، بنابراین سعی کنید مشخصات و اطلاعات خود را امن نگه دارید و تلاش کنید حساب‌های کاربری را که کمتر به آنها سر می‌زنید، ببندید. در پایان باید بگوییم که حفاظت از اطلاعاتتان مانند کلیدی برای حفظ آینده شماست. در عصر اینترنت که شرکت‌ها و همچنین مردم خود را در آن تبدیل به یک بازار اینترنتی برای معرفی به مشتریان بالقوه کرده‌اند، به‌طور قطع یک مساله تغییر کرده و آن تعیین و ایجاد تمایز بین زندگی شخصی و حرفه‌ای است. همان‌طور که اسکات مک‌نیلی از شرکت سان مایکروسیستمز به‌درستی گفت که: شما هیچ حریم خصوصی ندارید، پس به‌دنبال آن نباشید!

ترفند

بازگردانی ایمیل ارسال شده

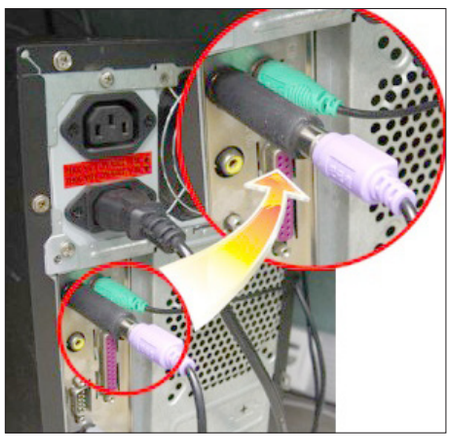
جیمیل ابزاری بسیار قدرتمند در دنیای مجازی است که شما می‌توانید قابلیت‌های آن را با فعال کردن افزونه‌های موجود در آزمایشگاه آن، افزایش دهید. اگر شما با این آزمایشگاه به‌تازگی آشنا شده‌اید، این یک موقعیت آزمایشی برای آشنایی با خصوصیات کاربردی‌تر جیمیل است. قابلیت‌هایی که از این آزمایش سربلند بیرون می‌آیند، به‌صورت یک قابلیت استاندارد برای جیمیل به کار برده می‌شوند اما تا زمانی که آنها در آزمایشگاه هستند، همیشه احتمال از کار افتادن، تغییر و یا حذفشان وجود دارد. برای فعال‌سازی قابلیت‌های آزمایشگاه جیمیل، به آیکون چرخ‌دنده در بالا و سمت چپ صفحه جیمیل مراجعه کرده و وارد تنظیمات شوید، سپس در سربرگ labs می‌توانید قابلیت‌های مورد نظرتان را با انتخاب گزینه فعال و ذخیره‌سازی تغییرات استفاده کنید. اگر در هنگام استفاده از هر کدام از این قابلیت‌ها دچار مشکل شدید، می‌توانید به راحتی به این آدرس، جیمیل خود را بازیابی کنید که در این صورت این قابلیت‌ها غیر فعال خواهند شد.

اگر شما قصد ارسال یک ایمیل با اظهار نظرهای تند و منتقدانه و یا ایمیلی از روی خشم و عصبانیت را دارید، معمولا پس از ارسال، احساس اضطراب ناشی از پشیمانی از ارسال آن ایمیل به سراغ شما می‌آید. اگر شما توانایی کنترل خود را در چنین موقعیت‌هایی ندارید، قابلیت بازگردانی ایمیل ارسال شده در آزمایشگاه جیمیل گزینه‌ای مناسب برای نجات شما از این موقعیت است.

این قابلیت، ایمیل‌های شما را با تاخیر ۵، ۱۰، ۲۰ و یا ۳۰ ثانیه ارسال می‌کند که با کلیک روی گزینه Undo به شما زمانی مناسب برای جلوگیری از ارسال پیامتان را خواهد داد. توجه داشته باشید هنگامی که این قابلیت را فعال کردید، کافی است زمان تاخیر را در سربرگ جنرال در تنظیمات مشخص کنید.

واژه‌نامه

کی‌لاگر (keylogger) چیست؟



کی‌لاگر (keylogger)، به نرم‌افزارهایی گفته می‌شود که کلیدهای فشرده‌شده روی صفحه کلید را ذخیره می‌کنند، به‌صورتی که می‌توان از آنها، اطلاعات تایپ شده کاربران از قبیل رمزهای عبور آنها را سرقت کرد. از کی‌لاگرها می‌توان برای یافتن منابع اشکالات استفاده کرد و نحوه ارتباط کاربران و سیستم و نحوه انجام کار و پیشرفت آن را در بعضی کارهای اداری مورد بررسی قرار داد. کی‌لاگرها به‌طور گسترده در اینترنت در دسترس هستند. کی‌لاگرها را می‌توان هم به‌صورت نرم‌افزاری و هم به‌صورت سخت‌افزاری مورد استفاده قرار داد. ابزارهای سخت‌افزاری عموما به سه شکل در دسترس هستند: ۱) ابزاری که به کابل صفحه‌کلید متصل می‌شود ۲) ابزاری که داخل صفحه‌کلید قرار می‌گیرد ۳) ابزاری که همانند قطعات معمول صفحه‌کلید است و جایگزین آنها می‌شود. نوع اول به‌راحتی قابل شناسایی و نصب است ولی نوع دوم و سوم نیاز به دسترسی بیشتر به صفحه کلید دارند و به‌راحتی قابل شناسایی نیستند.

یک روش ساده برای مقابله با کی لاگرها

اگر در یک کافی‌نت از اینترنت استفاده می‌کنید، برای جلوگیری از دزدیده شدن نام و گذرواژه‌هایتان به‌ازای هر حرفی که در فیلد کاربر یا گذرواژه تایپ می‌کنید، روی قسمت دیگری از صفحه کلیک کنید تا فوکوس از روی جعبه متن برداشته شود، سپس تعدادی کلید را به‌صورت تصادفی فشار دهید. پس از این کار، حرف بعدی از نام یا گذرواژه‌تان را وارد کنید. این کار را تا وارد کردن کامل مشخصات ادامه دهید. با انجام این روش ساده، آنچه در برنامه کی‌لاگر ذخیره می‌شود، تعداد زیادی حروف تصادفی است. گرچه اطلاعات شما نیز در این حروف قرار دارد اما کشف آنها بسیار مشکل است. این روش نمی‌تواند مانع کی‌لاگرهایی شود که در سطوح بالاتر فعالیت می‌کنند یا به‌صورت مستقیم مقادیر داخل فیلدها را می‌خوانند.

هولوگرام‌های همراه: آیا هولوگرافی آینده تلفن‌های همراه را رقم می‌زند؟

بامداد جنوب: سال ۱۹۷۷ زمانی که جورج لوکاس، کارگردان فیلم‌های جنگ ستارگان ایده جدیدی را برای انتقال صدا، تصویر و بعد ارائه کرد، کمتر کسی فکر می‌کرد این رویا به واقعیت تبدیل شود. برای تحقق این رویا کافی بود کودکان دوران فیلم‌های جنگ ستارگان، بزرگ شوند تا به رویای خود در زندگی امروز جان ببخشند. این رویای صادقه یعنی یافتن راهی برای به نمایش درآوردن تصویر، صدا و بعد به‌صورت معلق در هوا، هولوگرام نام گرفت. حالا این فناوری نوپا که هنوز هم چندان جدی گرفته نشده، راه خود را به تلفن‌های همراه باز کرده است. تصور این که در حال بازی فروت نینجا، میوه‌ها به جای حرکت در صفحه نمایش تلفن همراه، به‌سمت شما پرتاپ شوند یا آن که مدل سه بعدی ساختمان‌ها و ماشین‌های مختلف را روبه‌روی صورتتان تماشا کنید، هیجان‌انگیز به نظر می‌رسد اما این که این فناوری دقیقا چیست و آیا راهی برای ورود به تلفن‌های همراه دارد یا خیر، پرسشی است که در این گزارش به آن پاسخ می‌دهیم.

هولوگرام چیست؟

به بیان ساده می‌توان هولوگرام یا عمل هولوگرافی را روشی برای نمایش تصاویر سه بعدی دانست. در این روش که به آن «تمام‌نگاری» هم گفته می‌شود، به پرده نمایش یا رابطی مانند عینک‌های سه بعدی نیاز نیست و کاربر می‌تواند تصاویر را مقابل چشمانش و معلق در هوا ببیند. موضوع اصلی در تمام‌نگاری ایجاد بستری برای به تصویر در آوردن بدون نیاز به پرده نمایش است، زیرا ذرات فتون که از یک منبع نور ارسال می‌شود، پس از برخورد با یک جسم که آنها را انعکاس نمی‌دهد، مرئی می‌شوند. اکنون تلاش‌های زیادی برای نمایش‌های هولوگرامی انجام شده که یکی از متداول‌ترین آنها استفاده از هوا به‌صورت مه است. این هوای سنگین باعث می‌شود ذرات نور بستری برای نمایش پیدا کنند.

استفاده از هوای غلیظ یکی از کم‌هزینه‌ترین روش‌ها برای نمایش هولوگرام است، اما معمولا تصویر به دست آمده کیفیت قابل توجهی ندارد و با شدت غلظت این هوای سیال، کیفیت تصویر نیز کاهش پیدا می‌کند. علاوه بر این، ایجاد این هوای مه‌آلود که محدوده کمی برای نمایش ایجاد می‌کند، روش چندان مناسبی نیست تا بتوان آن را برای استفاده در منازل نیز به کار برد. استفاده از قطرات آب با دستور العملی مشابه اما کیفیتی مناسب‌تر روشی دیگر برای تمام‌نمایی است.

روش کارآمدتر اما بسیار پرهزینه برای نمایش تصاویر هولوگرام، استفاده از پرتوهای لیزری است. دانشمندان ژاپنی در یک پروژه بسیار پرهزینه با تعریف فاصله انفجار برای میلیون‌ها پرتوی لیزر توانستند هولوگرافی را بدون نیاز به بستری مانند پرده نمایش، هوای غلیظ و قطرات آب ایجاد کنند. البته یک نمایش ده ثانیه‌ای برای هولوگراف لیزری هزینه‌ای نزدیک به یک میلیون دلار دارد، برای همین به نظر نمی‌رسد هیچ‌وقت پای این شیوه به تولید انبوه و بازار برسد.

چینی‌ها دست به کار می‌شوند

ورود فناوری هولوگرام به تلفن‌های همراه به علت وجود دردسرهای موجود و فضای زیادی که نمایشگرهای تمام‌نما اشغال می‌کنند، شاید کمی بعید به نظر برسد اما به تازگی یک شرکت چینی ادعا کرده که اولین گوشی‌های هوشمند را با رابط هولوگرافی تولید کرده است. این تلفن همراه Estar Takee ۱ نام دارد و احتمالا بسیاری از اهالی دنیای فناوری حتی یک بار هم نام شرکت سازنده آن را نشنیده‌اند. این گوشی برای پردازش تصویر تمام‌نما از یک داک استفاده می‌کند که پشت گوشی سوار است. چهار دوربین نیز جلوی تلفن قرار دارند تا مسیر چشم کاربر را برای ایجاد یک تصویر سه بعدی تشخیص دهند.

طبق ادعای این شرکت در وبسایتش، این چهار دوربین ویژگی‌های متعددی دارند که به سیستم عامل تلفن همراه اجازه می‌دهند حرکات دست کاربر را نیز تشخیص دهد؛ یعنی مشابه اتفاقی که در کینکت مایکروسافت می‌افتد. با توجه به این ویژگی، کاربر می‌تواند کنترل کاملی بر تصاویر سه بعدی پیرامونش داشته باشد و کارهایی مانند باز کردن قفل گوشی، کار با صفحه لمسی و انجام بازی‌هایی که به‌دقت بالایی نیاز ندارند، امکان‌پذیر خواهد بود. این شاهکار چینی‌ها علاوه بر ویژگی منحصربه‌فردش، در گروه تلفن‌های همراه معمولی قرار می‌گیرد و با داشتن یک صفحه نمایش ۵/۵ اینچی، دوربین ۱۳ مگاپیکسلی و باتری ۲۵۰۰ میلی آمپر ساعتی باب دل کاربران نه چندان حرفه‌ای است. Takee از یک پردازنده MediaTek OCTA استفاده می‌کند و دو گیگابایت رم، حافظه ۳۲ گیگابایتی آن را پشتیبانی می‌کند. این تلفن همراه که قرار است فقط در چین به فروش برسد، در دو رنگ سیاه و سفید به بازار عرضه می‌شود.

با توجه به نشانه‌های موجود باید نزدیک‌ترین رقیب Estar Takee ۱ را آمازون دانست و باید منتظر ماند تا این پروژه به مرحله تولید برسد. آمازون برای اجرای قابلیت تمام‌نمایی خود قرار است از هر دو ویژگی شناسایی مسیر مردمک چشم و همچنین ایجاد هوای غلیظ استفاده کند. اکنون مشکل اصلی جای دادن تمام این امکانات در بدنه اصلی تلفن همراه است، بدون آن که جای بیش از حدی اشغال کند یا وزن گوشی را از حد انتظار بالاتر ببرد.

بررسی

چگونه آنتی‌ویروسی مناسب انتخاب کنیم؟

محسن رسولی

در این مقاله سعی شده است تا در حد امکان به بررسی شیوه‌ها و معیارهای انتخاب آنتی‌ویروس مناسب بپردازیم. معیارهای مورد بررسی شامل سرعت عملکرد، نصب سریع و محیط کاربری ساده، وضعیت آپدیت شدن و مانند آن است.

تاثیر گذاری آنتی‌ویروس بر سرعت سیستم کاربر

برای بسیاری از کاربران، به‌خصوص آن دسته از کاربرانی که کامپیوتر آنها کمی قدیمی شده، این مساله مهم است که آنتی‌ویروس نصب شده، سبب کندی عملکرد سیستمشان نشود اما نباید فراموش کرد که هدف اصلی از نصب آنتی‌ویروس، ایجاد و حفظ امنیت است. با این حال، سرعت عالی و برقراری امنیت عالی در کنار یکدیگر، شدنی نیست. طبیعی است که وقتی آنتی‌ویروسی برای محافظت از سیستم شما، درگیر پیاده‌سازی روش‌های تعریف شده‌اش است، مقادیری از منابع CPU شما را اشغال می‌کند و این امر، کندی نسبی سرعت سیستم را به‌دنبال خواهد داشت. البته این مساله، بیشتر درباره کامپیوترهای قدیمی صدق می‌کند، زیرا کامپیوترهای امروزی که CPU آنها از تکنولوژی Core بهره‌مند هستند، کمتر دچار افت سرعت می‌شوند، بنابراین بهتر است به‌جای تمرکز روی کاهش سرعت سیستم، روی برقراری یک امنیت کامل متمرکز شوید.

نصب سریع و محیط کاربری ساده

دسترسی سریع به بخش‌های مختلف یک آنتی‌ویروس و تنظیمات ساده و کاربرپسند، یکی از گزینه‌هایی است که سبب محبوبیت آنتی‌ویروس در میان کاربران می‌شود. البته این پارامتر، یک پارامتر تعیین کننده برای انتخاب یک آنتی‌ویروس نیست و نسخه‌های امروزی، تقریبا امکان و گزینه‌های مشابهی دارند.

دفعات آپدیت شدن در طول روز و حجم دانلود شده

برای کاربران، آنتی ویروسی مناسب است که تعداد دفعات آپدیت و مقدار حجم دریافتی، کم باشد تا هم ترافیک اینترنت کمتری مصرف شود و هم زمان کمتری داشته باشد. البته اگر کاربران در سرعت و ترافیک مصرفی اینترنت، مشکل یا محدودیتی نداشته باشند، این پارامتر نباید در انتخاب آنتی‌ویروس مناسب، برجسته شود.

سرعت اسکن کردن کل سیستم (Full System Scan)

تکنولوژی Scanning در آنتی‌ویروس‌ها مشابه است اما تفاوت‌هایی نیز دارد. سرعت جست‌وجو و آنالیز فایل‌ها، پارامتری است که می‌تواند مشغولیت CPU را رقم بزند. بسیاری از آنتی‌ویروس‌ها به گونه‌ای هستند که اگر هنگام اسکن فعالیت دیگری روی سیستم انجام دهید، به‌طور قطع به مشکل برخواهید خورد و با کاهش سرعت شدید مواجه خواهید شد که توصیه می‌شود این کار را انجام ندهید. تکنولوژی Silent Scanning برای زمانی است که وقتی شما با کامپیوتر کار نمی‌کنید، به‌طور اتوماتیک به راه می‌افتد و سیستم شما را اسکن خواهد کرد. سرعت بررسی فایل‌های شما به حجم، نوع و تعداد فایل‌ها نیز بستگی دارد. برای مثال، اسکن تصاویر، موزیک و ویدئوها خیلی سریع‌تر از فایل‌های DLL و یا فایل‌های اجرائی صورت می‌گیرد.

شناسایی خودکار Flash Memory پس از اتصال به درگاه USB

تکنولوژی Auto-Detection یکی از قابلیت‌های جدید آنتی‌ویروس‌هاست که بسیار مفید و کارساز است. امروزه اغلب آلودگی‌ها از طریق Flash Memory ها منتشر می‌شوند. آنتی‌ویروسی مناسب است که بلافاصله پس از متصل کردن Removable Disk‌ها بتواند آن را تشخیص داده و پیش از استفاده کاربر، اقدام به اسکن کند. بعضی از آنتی‌ویروس‌ها این قابلیت را دارند و به‌محض اتصال Flash Memory، از قسمت Notification Area (کنار ساعت کامپیوتر)، پنجره‌ای باز می‌شود و از شما می‌خواهد که سخت‌افزار متصل شده را اسکن کنید. این Pop-Up بسیار مناسب است، زیرا اگر نباشد ممکن است کاربر فراموش کند که پیش از استفاده از سخت‌افزار، آن را اسکن کند. بعضی آنتی ویروس‌ها این قابلیت را دارند ولی فعال نیستند و شما باید در تنظیمات آنتی‌ویروس، تیک Enable را فعال کنید. پاره‌ای دیگر از آنتی‌ویروس‌ها، به این سرویس، مجهز نیستند

معیار نخست برای انتخاب آنتی‌ویروس مناسب، ایجاد امنیت و سپس کاهش نیافتن سرعت سیستم کاربر است. نوع استفاده کاربران از کامپیوترشان، سرعت اینترنتی که در اختیار دارند و همچنین توانمندی سخت‌افزاری کامپیوترشان، عوامل اصلی در انتخاب یک آنتی‌ویروس مناسب است. کاربرانی که کارهای Render گیری (طراحی پیشرفته و خروجی با کیفیت و ابعاد بالا) انجام می‌دهند، نباید آنتی‌ویروسی انتخاب کنند که منابع زیادی از CPU را اشغال کند، زیرا در کارشان اختلال ایجاد می‌کند. کاربرانی که اغلب وقت خود را به بازی، وبگردی و یا شنیدن موزیک می‌گذرانند، تقریبا می‌توانند هر آنتی‌ویروسی را انتخاب کنند (به شرط سرعت اینترنت مناسب و قدرت بالای سخت‌افزارهای کامپیوترشان). در نهایت، به کاربران توصیه می‌شود که کندی سرعت را تحمل کرده و آنتی‌ویروسی را انتخاب کنند که تضمین کننده حداکثر امنیت باشد، چراکه هدف اصلی از نصب آنتی‌ویروس، همین است.