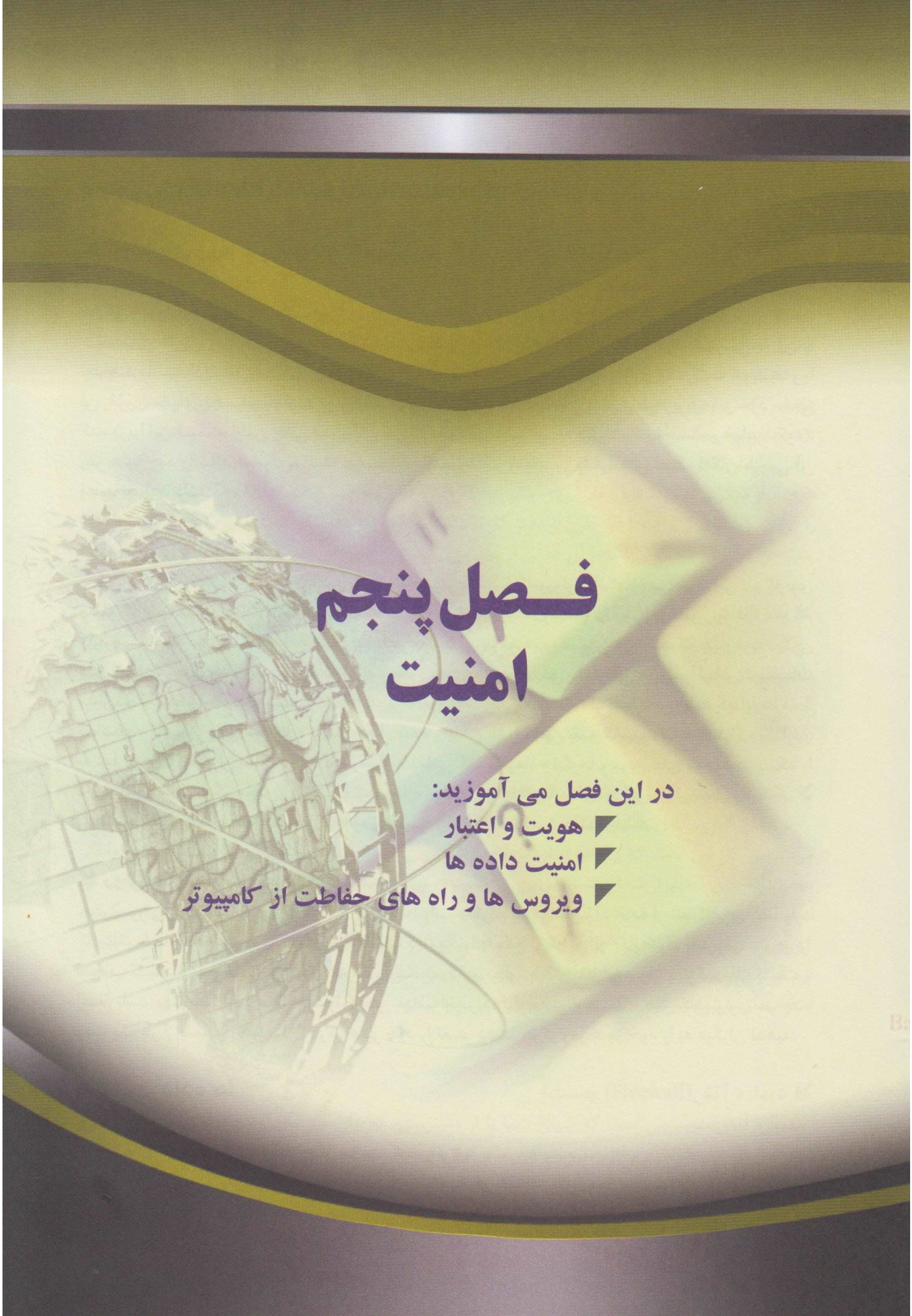
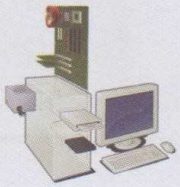


فصل پنجم
امنیت

در این فصل می آموزید:

- هویت و اعتبار
- امنیت داده ها
- ویروس ها و راه های حفاظت از کامپیوتر



هویت(Identity)/ اعتبار(Authentication)

نام کاربری و رمز عبور ورود به کامپیوتر

رمز عبور:

با تعیین کردن رمز عبور برای کامپیوتر، سایر کاربرانی که رمز را نمی دانند، اجازهٔ دسترسی به آن را نخواهند داشت. لذا نباید رمز عبور خود را به کسی بدهید. هرگز رمز عبور خود را روی یک کارت ننویسید و یا آن را روی مانیتور نچسبانید و مهم تر از همه هیچ وقت سعی نکنید که آن را در سطح زیرین میز خود مخفی کنید(زیرا این قسمت، اولین جایی است که مجرمان به منظور دستیابی به سیستم شما جستجو خواهند کرد). رمز عبور خود را نباید فراموش کنید؛ در بسیاری از موارد اگر رمز عبور را فراموش کنید، امکان بازیابی آن وجود نخواهد داشت.

نام کاربری و رمز عبور:

از نام کاربری معمولاً برای وارد شدن به یک کامپیوتر یا شبکهٔ کامپیوتری استفاده می شود. این نام کاربری متعلق به شماست و هویت شما را در شبکه تعریف می کند. به علاوه شما از یک رمز عبور نیز در کنار نام کاربری استفاده می کنید که فقط شما آن را می دانید. این رمز عبور تضمین می کند که هیچ فرد دیگری نمی تواند به جای شما وارد شبکه شود. به محض ورود به شبکه، حق دسترسی هایی بر اساس تصمیمات مدیر شبکه به شما داده می شود. هدف از تعیین حقوق دسترسی افراد در یک شبکه این است که آن ها فقط بتوانند به کامپیوترهایی که اجازه دارند متصل شده و یا آن ها را مابین بقیه کامپیوترها به اشتراک بگذارند. به عبارت دیگر، مدیران شبکه اجازهٔ دسترسی به تمامی کامپیوترها، چاپگرها و مودم های موجود در شبکه را دارند. اما از طرف دیگر ممکن است شما تنها اجازه استفاده از چاپگرهای خاصی که برایتان تعیین شده است را داشته باشید یا فقط به داده های محدود و معینی از شبکه دسترسی داشته باشید.

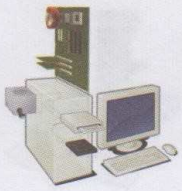
روش های انتخاب رمز عبور

در صورتی که فرد دیگری خود را به جای شما وانمود کرده و بخواهد با استفاده از نام کاربری شما وارد کامپیوتر شما شود، رمز عبور شما چیزی است که می تواند مانع از انجام این کار شود. باید رمز عبوری را انتخاب کنید که به راحتی نتوان آن را حدس زد. معمولاً رمز عبور باید حداقل ۸ حرف و ترکیبی از کلمات و اعداد باشد. بهتر است رمز عبور خود را به طور منظم تغییر دهید. بعضی از سیستم های کامپیوتری هر چند وقت یک بار از شما می خواهند که رمز عبور خود را تغییر دهید. هرگز رمز عبور خود را به دیگران ندهید.

امنیت داده ها

پشتیبان گیری داده ها خارج از سایت کامپیوتری

گرفتن پشتیبان و نگهداری آن در نزدیکی کامپیوتر به هیچ وجه روش خوبی نیست؛ اگر فردی کامپیوتر



شما را بدزدد، احتمالاً پشتیبان های شما را نیز به سرقت خواهد برد. اگر آتش سوزی رخ دهد ممکن است پشتیبان‌ها نیز از دست بروند. بنابراین لازم است که پشتیبان را در جایی امن و دور از کامپیوتر نگهداری کنید. بهترین کار این است که پشتیبان را در یک صندوق ضد حریق نگهداری کرد.

لزوم گرفتن نسخه پشتیبان چیست؟

مهمترین چیزی که در کامپیوتر دارید، اطلاعات شماست. معمولاً محتوای روی دیسک سخت، نتیجهٔ چندین سال کار است. اگر دیسک سخت روزی دچار مشکل شود، شما اطلاعات تمام این سال ها را از دست می دهید. به همین دلیل، لازم است به طور منظم از اطلاعات روی کامپیوتر، پشتیبان گیری کنید. در سازمان های بزرگ، پروسهٔ پشتیبان گیری معمولاً توسط تیم پشتیبانی کامپیوتر و به صورت خودکار انجام شده و داده ها بر روی یک کامپیوتر مرکزی متصل به شبکه نگهداری می شوند.

در سازمان های کوچکتر، اشخاص خودشان اقدام به گرفتن نسخه پشتیبان از اطلاعاتشان می کنند. اگر هیچ ابزار دیگری ندارید، فایل ها را روی یک حافظهٔ فلش USB یا دیسکCD یا DVD کپی کنید و آن ها را دور از کامپیوتر و ترجیحاً در خارج از دفتر کار نگهداری کنید. اگر دفتر کار شما آتش بگیرد و دیسک های پشتیبان در کنار کامپیوتر باشند، آن ها نیز از بین می روند.

سازماندهی کامپیوتر برای پشتیبان گیری بهتر

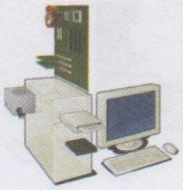
اگر خوب فکر کنید متوجه می شوید که کامپیوتر شما حاوی برنامه های نصب شده زیاد و همچنین داده های زیادی است که توسط آن ها ایجاد کرده اید. شما تنها لازم است که از داده ها پشتیبان گیری کنید نه از نرم افزارها. اگر یک پوشه درست کنید و داده ها را در آن قرار دهید، فقط کافی است که از این دایرکتوری(Directory) پشتیبان بگیرید.

پشتیبان گیری کامل و پشتیبان گیری افزایشی

پشتیبان گیری کامل به این معناست که شما از تمام داده های داخل کامپیوتر نسخه پشتیبان تهیه کنید. مزیت این کار این است که از تمام اطلاعات موجود بر روی دیسک سخت پشتیبان گرفته می شود، اما اگر حجم داده های کامپیوتر شما زیاد باشد، این کار بسیار زمانبر خواهد بود. پشتیبان گیری افزایشی به این معنی است که شما هر هفته یک پشتیبان گیری کامل انجام دهید، اما هر شب فقط از فایل هایی پشتیبان بگیرید که به تازگی آن ها را ایجاد و یا ویرایش کرده اید و به این ترتیب در وقت صرفه جویی کنید. با استفاده از نرم افزار مناسب، این پروسه پشتیبان گیری اتوماتیک می شود و معمولاً تنها کاری که شما باید انجام دهید انتخاب کردن نوع پشتیبان گیری کامل یا افزایشی خواهد بود.

دیواره آتش(Firewall) چیست؟

دیواره آتش سیستمی است که شبکهٔ شما را از دسترسی کاربران غیر مجاز محافظت می کند. دیواره آتش می تواند از طریق نرم افزار، سخت افزار یا ترکیبی از هر دو پیاده سازی شود. اگر برای اتصال به اینترنت از اتصال باند پهن استفاده می کنید، استفاده از یک دیواره آتش برای جلوگیری از ورود افراد سودجو به قصد



هک کردن کامپیوتر شما امری حیاطی است.

مسائل مربوط به سرقت داده ها

شما باید چند مورد را برای جلوگیری از به سرقت رفتن داده های کامپیوترتان رعایت کنید. این موارد در نکات زیر آورده شده است:

نام کاربری و رمز عبور:

همیشه از نام کاربری و رمز عبور برای دسترسی به کامپیوتر استفاده کنید.

محافظت فیزیکی از کامپیوتر:

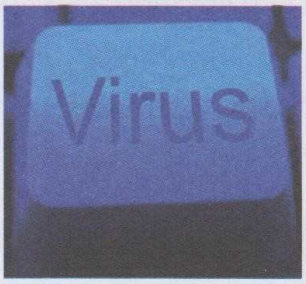
برای حفاظت فیزیکی از کامپیوتر و ادوات جانبی آن می توانید از کابل های مخصوص همراه با قفل که کامپیوتر را بر روی میز قفل می کنند استفاده کنید. البته این کار باعث محافظت از خود کامپیوتر می شود و نه محافظت از اطلاعات حساس روی کامپیوتر.

اگر لپ تاپ شما دزدیده شود چه اتفاقی می افتد؟

اگر هیچ رمز عبوری بر روی کامپیوتر خود نداشته باشید، تمام داده های روی آن در خطر هستند. همین خطر برای اسناد مهم یا حساس نیز وجود دارد؛ اگر هر یک از آن ها به تنهایی دارای رمز حفاظتی نباشند، ممکن است در معرض خطر قرار گیرند. اگر در یک سازمان بزرگ کار می کنید، همیشه بخش پشتیبانی فنی سازمان را از این گونه مسائل با خبر کنید.

ویروس ها

ویروس های کامپیوتری



ویروس ها برنامه های کوچکی هستند که خود را در دیسک ها (هم در دیسکت ها و هم در دیسک سخت) پنهان می کنند. شما هنگامی از وجود ویروس ها در کامپیوترتان مطلع می شوید که آن ها فعال شده باشند، مگر اینکه کامپیوتر شما دارای نرم افزار ضد ویروس باشد. ویروس های مختلف به روش های مختلفی فعال می شوند.

> ویروس ها می توانند تمام داده های شما را از بین ببرند.

نکات مربوط به آلودگی به ویروس

ویروس ها در دیسک پنهان می شوند و هنگامیکه وارد دیسک (دیسکت یا دیسک سخت) می شوید برنامهٔ ویروس شروع به کار کرده و کامپیوتر شما را آلوده می کند. بدترین نکته این است که ویروس کامپیوتری می تواند از یک کامپیوتر به کامپیوتر دیگر منتقل شود که این امر ممکن است از راه استفاده از دیسک های آلوده به ویروس و یا از راه شبکه انجام گیرد. اینترنت به شما اجازهٔ دسترسی به فایل ها از سراسر دنیا را می دهد و شما به هیچ وجه نباید بدون داشتن برنامهٔ ضد ویروس به اینترنت متصل شوید. همچنین همیشه باید

آن را به روز رسانی کنید. اگر روی کامپیوتر شما یک برنامه ضد ویروس به روز رسانی نشده وجود دارد، مثل این است که شما اصلاً برنامه ضد ویروس روی کامپیوترتان ندارید. بسیاری از برنامه های ضد ویروس مثل Norton، امکان به روز رسانی بانک ویروس یابی نرم افزار را فراهم می کنند و پس از به روز رسانی، برنامه می‌تواند ویروس هایی که به تازگی ساخته شده اند را پیدا کرده و آن ها را از بین ببرد.

اطلاعات بیشتر :

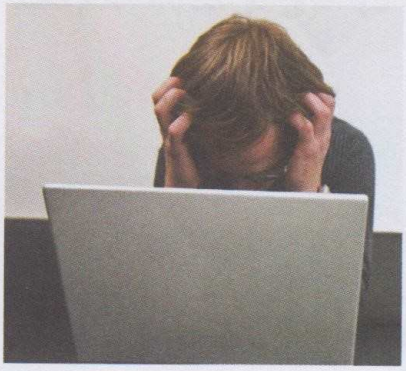
McAfee Anti–virus software	http://www.macafee.com
Norton Anti–virus software	http://www.symantec.com/avcenter
AVG Anti–virus software	http://www.grisoft.com

محافظت از کامپیوتر در مقابل ویروس

امن ترین روش استفاده از کامپیوتر این است که به شبکه های محلی و یا اینترنت وصل نشوید. در این حالت کامپیوتر شما مستقل(Stand Alone) است. بعلاوه اگر دیسک هایی را که در کامپیوترهای دیگر استفاده شده اند، در این کامپیوتر قرار ندهید، این کامپیوتر در مقابل هر نوع نفوذ و حمله ای از طرف ویروس ها مصون خواهد بود.

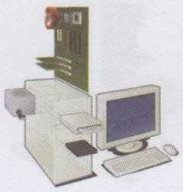
متأسفانه امکان اتصال به سایر کامپیوترها یا در واقع اتصال به اینترنت، کامپیوترهای امروزی را به ابزارهایی پرکاربرد و مفید تبدیل کرده است.

همیشه مطمئن شوید که برای دسترسی به تمام کامپیوترها نام کاربری و رمز عبور درخواست می شود. و اینکه همه کدهای نرم افزاری کمکی امنیتی (Security Patch) که مایکرو سافت ارائه کرده است، روی کامپیوترها اعمال شده باشند.



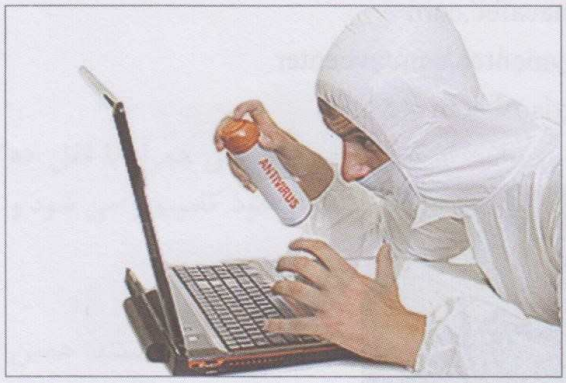
تعداد کاراکتر های رمز عبور باید به قدر کافی بوده و در آن ها هم از اعداد و هم از حروف به صورت ترکیبی استفاده شده باشد. همچنین باید رمز عبور مرتباً در فواصل زمانی مشخص عوض شود.

بسیاری از افراد از رمزهای عبوری استفاده می کنند که به امور شخصی آن ها مربوط می شود. مثلاً نام همسر یا نام حیوانات خانگی خود را انتخاب می کنند. حدس زدن این اسامی برای یک هکر حرفه‌ای بسیار آسان است. اگر شما برای ورود به بخش های مختلف کامپیوتر،



رمزهای عبوری زیادی تعریف کرده باشید، بالعکس ممکن است که امنیت کامپیوتر کاهش یابد، چراکه به دلیل تعداد زیاد رمز عبور، شما ناچار هستید لیستی از آن ها را در کشوی میزتان داشته باشید تا آن ها را فراموش نکنید و این امر کل بخش های کامپیوتر را در معرض خطر قرار می دهد. در صورت فراموش کردن رمز عبور دسترسی به شبکه، مدیر شبکه باید بتواند یک رمز عبور جدید به شما بدهد.

اگر ویروسی را بر روی کامپیوتر خود پیدا کردید باید چه کنید؟



اگر متوجه وجود ویروس بر روی کامپیوتر شدید، نگران نشوید. اگر نرم افزار ضد ویروس، شما را از وجود یک ویروس آگاه کرد، این احتمال وجود دارد که نرم افزار، قبل از ویروسی شدن کامپیوتر و آسیب رسیدن به آن، ویروس را یافته باشد. مثلاً اگر دیسکی را در کامپیوتر قرار دهید، برنامهٔ ضد ویروس به طور خودکار دیسک را اسکن می کند. اگر دیسک ویروس داشته باشد، پیامی نمایش داده می شود و به شما هشدار می دهد که دیسک ویروسی است و نرم افزار باید به صورت خودکار، ویروس را پاک کند. روش متداول دیگر برای آلوده شدن به ویروس از طریق پست الکترونیکی است.

اگر در یک شرکت بزرگ کار می کنید، احتمالاً یک گروه پشتیبانی IT دارید که می توانند کامپیوتر شما را از دست ویروس ها نجات دهند.

محدویت های نرم افزار ضد ویروس

نرم افزار ضد ویروس فقط ویروس هایی را پیدا می کند که آن ها را می شناسد. بنابراین باید نرم افزار ضد ویروس خود را به روز رسانی کنید تا بتواند ویروس های جدیدی را که دائماً در حال تولید هستند، پیدا کند.