تمرین

۱ - یک حساب پست الکترونیک در سایت **www.Gmail.com** برای خود ایجاد نمایید.
۲ - آدرس پست الکترونیک خود را در برنامه **Outlook Express** معرفی نمایید.
۳ - نامه‌ای ایجاد نموده و سپس آن را به صورت موقت در پوشه **Draft** ذخیره کنید.
۴ - نامه ایجاد شده در پوشه **Draft** را به آدرس پست الکترونیک هم کلاسی خود ارسال کنید.
۵ - یک امضاء خودکار تعریف کرده و نامه جدیدی را به آدرس پست الکترونیک هم کلاسی خود ارسال کنید.
۶ - نامه‌های خود را دریافت و ارسال کرده و کاری کنید که از اینترنت به صورت اتوماتیک قطع شوید.
۷ - نامه ای به دوست خود ارسال کنید و یک فایل تصویر به صورت ضمیمه همراه آن ارسال کنید.
۸ - نامه‌های خود را در **Inbox** برحسب تاریخ و ساعت دریافت نامه مرتب نمایید.
۹ - نام و نام خانوادگی و آدرس پست الکترونیک شش نفر از دوستان خود را در کتاب آدرس‌ها تعریف کنید.
۱۰ - گروهی به نام **BestFreinds** ساخته و سه نفر از دوستان نزدیک خود را به عضویت آن درآورید.
۱۱ - نامه‌ای را تهیه کرده و به همه اعضاء گروه **BestFreinds** ارسال نمایید.
۱۲ - نامه جدیدی تهیه کرده و در قسمت **TO** آدرس پست الکترونیک خودتان و در قسمت **CC**، گروه **BestFreinds** را قرار دهید. بررسی کنید که دوستانتان پس از دریافت نامه می‌دانند که به غیر از خودشان - این نامه به چه افراد دیگری ارسال شده است؟
۱۳ - نامه دیگری ارسال کنید و در قسمت **TO** آدرس پست الکترونیک خودتان و در قسمت **BCC** گروه **BestFreinds** را قرار دهید. آیا باز هم دوستانتان می‌توانند دریافت کنندگان نامه را تشخیص دهند؟
۱۴ - پوشه‌های زیر را ایجاد نموده و در هر کدام دسته‌ای از نامه‌های **Inbox** خود را قرار دهید.

- **Important**
- **Class**
- **Friends**

۱۵ - پوشه **Class** را به نام **Work** تغییر نام دهید.
۱۶ - پوشه **Important** را حذف نمایید.
۱۷ - کاری کنید که لیست **Deleted items** در هنگام خروج از برنامه خالی گردد.

۱۸ - یکی از نامه‌های درون پوشه **Friend** را به طور کامل حذف نمایید.

۱۹ - کاری کنید از این پس با حذف هر نامه، آن نامه به طور کامل حذف گردد و درون پوشه **Deleted items** قرار نگیرد.

۲۰ - نامه‌هایی که در پوشه **Inbox** قرار دارند و متن **Dear** درون آنها به کار رفته و دارای علامت پرچم می‌باشند را جستجو کنید.

۲۱ - نامه‌هایی که ضمیمه دارند را بیابید.

۲۲ - یک آدرس پست الکترونیک در سایت **Yahoo** ایجاد کنید و تحقیق کنید که چگونه می‌توان از **Outlook Express** برای ارسال و دریافت نامه‌های **Yahoo** استفاده کرد.

آزمون تشریحی

۱ - پست الکترونیک چیست؟ مزایای آن چیست؟

۲ - آدرس پست الکترونیک از چه از چه اجزایی تشکیل شده است؟ توضیح دهید.

۳ - پروتکل های دریافت و ارسال پست الکترونیک را توضیح دهید.

۴ - کاربرد پوشه های **Inbox**، **Outbox**، **Send Item** و **Draft** را شرح دهید.

۵ - در هنگام ایجاد نامه ، در چه شرایطی لیست **From** نمایش داده می‌شود؟

۶ - اولویت نامه به چه معنی است؟ انواع اولویت‌ها را نام ببرید.

۷ - معایب نامه‌های گرافیکی چیست؟

۸ - اصطلاحات **Reply**، **Reply All** و **Forward** را شرح دهید.

۹ - **Spam** چیست؟ توضیح دهید.

آزمون چهارگزینه‌ای

۱ - با فشردن کدام دکمه می‌توان از نرم‌افزار **Outlook Express** بدون اتصال به اینترنت استفاده نمود؟

الف) Work Offline ب) Outlook Express ج) Connect د) Setting

۲ - اگر بخواهیم نامه دریافت شده را برای افراد دیگری بفرستیم از کدام دکمه استفاده می‌کنیم؟

الف) Forward ب) Work Offline ج) Reply all د) Send

۳- هرگاه نامه‌ای را ارسال نمایم ابتدا در پوشه ..... و پس از ارسال به پوشه ..... انتقال می‌یابد.

الف) Outbox - Inbox ب) Sent Items - Outbox

ج) Outbox - Draft د) Outbox - Sent Items

۴- پوشه Outbox شامل .....

الف) لیست نامه‌های دریافت شده است. ب) لیست نامه‌هایی است که قرار است ارسال گردد.

ج) لیست نامه‌های حذف شده است. د) لیست نامه‌های ارسال شده است.

۵- اگر بخواهیم انتخاب کنیم که با کدام آدرس پست الکترونیکی خود نامه را می‌خواهیم ارسال کنیم از کدام گزینه استفاده می‌کنیم؟

الف) Address Book ب) Create Mail ج) From د) Send box

۶- برای ارسال نامه‌ای که گیرندگان دیگر از آن بی‌اطلاع باشند آدرس آن را در کنار ..... می‌نویسیم.

الف) BC ب) CC ج) Bcc د) To

۷- برای ارسال رونوشتی از نامه خود به اشخاص دیگر آن را در کنار متنی ..... می‌نویسیم.

الف) To ب) CC ج) Subject د) هیچکدام

۸- برای ارسال نامه از کدام گزینه استفاده می‌کنیم؟

الف) Alt + S ب) منوی File گزینه Send Message

ج) دکمه Send در نوار ابزار د) همه موارد

۹- با فشردن دکمه Send Later .....

الف) نامه به درون پوشه Draft می‌رود. ب) نامه به درون پوشه Outbox می‌رود.

ج) نامه به درون پوشه Inbox می‌رود. د) نامه به درون Address Book می‌رود.

۱۰- الصاق یک فایل به نامه برای ارسال را ..... می‌گویند.

الف) Send ب) Receive ج) Attachment د) Recipients

۱۱- برای استفاده از آدرس‌های Address Book در پنجره New Message روی ..... کلیک می‌کنیم.

الف)  ب)  ج)  د) 

۱۲- برای تهیه نامه به صورت گرافیکی از کدام گزینه منوی Format استفاده می‌کنیم؟

الف) Plain Text ب) Rich Text (HTML) ج) Graphic د) Theme

۱۳ - با انتخاب گزینه Save از منوی فایل نامه شما در ـــــــ ذخیره می‌شود.

الف) My Document ب) Outbox ج) Draft د) Inbox

۱۴ - کدامیک از نمادهای زیر نشان دهندهٔ داشتن فایل الصاقی است؟

الف) ۳ ب) ! ج) ۩ د) ↓

۱۵ - برای پاسخ به فرستنده یک نامه از کدام دکمه استفاده می‌کنید؟

الف)  ب)  ج)  د) 

۱۶ - Spam ـــــ

الف) به نامه‌های افراد مزاحم گویند.

ب) به نامه‌ای که چند بار به صورت متوالی از طرف افراد ناشناس فرستاده شود.

ج) به ویروس‌های اینترنتی می‌گویند.

د) موارد الف و ب صحیح است.

۱۷ - کدامیک از پوشه‌های زیر فایل حذف می‌باشد؟

الف) Inbox ب) Deleted Item ج) Important د) Outbox

۱۸ - در نرم افزار Outlook Express هرگاه پوشه‌ای را حذف نمایید آن پوشه به پوشه ـــــ انتقال می‌یابد.

الف) Recycle Bin ب) Outbox ج) Trash د) Deleted Items

۱۹ - در کادر گزینه To در پنجره Find ـــــ

الف) براساس آدرس فرستنده جستجو می‌کنیم.

ب) براساس آدرس گیرندگان جستجو می‌کنیم.

ج) براساس موضوع جستجو می‌کنیم.

د) موارد الف و ب صحیح است.

فصل نهم

ویروس‌های رایانه‌ای

هدفهای رفتاری :

پس از مطالعه این فصل از فراگیر انتظار می رود که :

- ☑ برنامه‌های مخرب را تعریف نماید و انواع آن را نام ببرد.
- ☑ راههای انتقال برنامه‌های مخرب را توضیح دهد.
- ☑ ویروس رایانه‌ای را تعریف نماید.
- ☑ انواع ویروس از نظر محل تاثیر گذاری را نام ببرد.
- ☑ روش‌های انتقال ویروس به رایانه را نام ببرد.
- ☑ راههای تشخیص ویروسی شدن سیستم را نام ببرد.
- ☑ روشهای مقابله با ویروسی شدن سیستم را نام ببرد.
- ☑ ویروس اینترنتی و روش‌های انتشار و مقابله با آن را شرح دهد.
- ☑ نرم‌افزار ضد ویروس را تعریف کند و با چند نمونه از آنها آشنا باشد.
- ☑ روش‌های مقابله نرم‌افزارهای ضد ویروس با ویروس‌ها را شرح دهد.
- ☑ نرم‌افزار Norton Antivirus را نصب نماید.
- ☑ قسمتهای مختلف نرم‌افزار Norton Antivirus را نام برده و کاربرد هر یک را توضیح دهد.
- ☑ عملیات ویروس‌یابی را با Norton Antivirus انجام دهد.
- ☑ نرم‌افزار Norton Antivirus را از طریق اینترنت بروزرسانی نماید.

زمان نظری : ۴ ساعت

زمان عملی : ۱۳ ساعت

۱-۹ آشنایی با برنامه‌های مخرب و انواع آن

هر نرم‌افزار با توجه به دستورالعمل‌هایی که در آن وجود دارد، عملیات خاصی را انجام می‌دهد. برنامه‌نویس یک نرم‌افزار با توجه به هدفی که از ایجاد نرم‌افزار دارد، یکسری دستورالعمل‌هایی را در نرم‌افزار پیش‌بینی می‌کند. حال اگر یک برنامه نویس قصد داشته باشد برنامه‌ای تولید کند که به برنامه‌های دیگر و فایلها و اطلاعات رایانه آسیب برساند، در نرم‌افزار یکسری دستورالعمل را برای نابود کردن و یا خراب کردن فایل‌های رایانه قرار می‌دهد.

برنامه‌های مخرب با اهداف مختلفی تولید می‌شوند. گاهی اوقات یک برنامه مخرب برای ضربه زدن به شرکتهای رقیب نرم‌افزاری و بدنام کردن محصولات شرکت رقیب تهیه می‌شود. گاهی اوقات برنامه مخرب توسط برنامه‌نویسان حرفه‌ای برای ضربه زدن به اطلاعات شبکه‌های رایانه‌ای کشورهای دیگر و یا نشان دادن قدرت نرم افزاری خود و مطرح کردن نام یک گروه در دنیای برنامه‌نویسان می‌باشد.

برنامه‌های مخرب را از لحاظ نوع عملکرد می‌توان به چهار دسته زیر تقسیم کرد :

- **کرم (Worm)**

برنامه‌ای که بدون اطلاع کاربران خود را بین رایانه‌ها تکثیر می‌کند. همچنین ممکن است این برنامه خود را در حافظه رایانه اینقدر تکثیر کند که رایانه دچار اختلال شود. کرم ممکن است به اطلاعات رایانه نیز آسیب برساند. کرم‌ها بیشتر در شبکه‌های رایانه‌ای و اینترنت امکان فعالیت دارند و از نقاط ضعف سیستم‌عامل‌ها و شبکه‌ها برای تکثیر خود استفاده می‌کنند.

- **اسب تراوا یا جاسوس (Trojan)**

برنامه‌ای که ظاهری مفید از خود نشان می‌دهد ولی در پشت صحنه عملیات مخربی را انجام می‌دهد یا اطلاعات کاربر را از طریق اینترنت در اختیار طراح برنامه قرار می‌دهد. مثلاً ممکن است این نرم‌افزار به صورت یک بازی در اختیار کاربر قرار گیرد ولی بعد از اجرا خود را در **Startup** قرار داده و هر بار که ویندوز اجرا می‌شود در حافظه قرار گیرد و اطلاعات مهم کاربر را به سرقت ببرد. (انتخاب اسم اسب تراوا برای این نوع برنامه‌های مخرب ، اشاره به داستان تاریخی اسب چوبی که یونانیان در جنگ از آن برای فریب دشمن استفاده کردند، دارد.)

- **بمب (Bomb)**

برنامه‌ای است که در آن کد مخربی گنجانده شده است که در حالت عادی این کد اجرا نمی‌شود ولی به محض اینکه شرایط مورد نظر نویسنده برنامه ایجاد شد ، کد مخرب اجرا شده و برنامه‌ها آسیب می‌بینند. مثلاً هر وقت زمان رایانه به تاریخ مشخصی برسد ، قسمت مخرب برنامه به کار می‌افتد به همین علت نام بمب را به این نوع برنامه‌ها نسبت می‌دهند.

- ویروس (Virus)

ویروس اصطلاح رایجی است که به همه برنامه‌های مخرب گفته می‌شود. در صورتیکه ویروس از نظر کارشناسان امنیتی تعریف مشخصی دارد که در ادامه با آن آشنا می‌شویم.

۹-۲ آشنایی با راههای انتقال برنامه‌های مخرب

برنامه‌های مخرب را همانند دیگر برنامه‌های رایانه‌ای از طرق مختلفی می‌توان بر روی رایانه‌ها منتقل کرد. ولی اگر دریافت کننده این برنامه بداند که ممکن است این برنامه مخرب باشد آن را اجرا نمی‌کند. به همین منظور تهیه کنندگان برنامه‌های مخرب ، سعی می‌کنند این برنامه‌ها را بدون اطلاع کاربران روی رایانه آنها منتقل کرده و اجرا کنند و یا اینکه به روشهای مختلفی اطمینان کاربران رایانه را جلب کنند و برنامه‌های مخرب را برنامه‌ای مفید و سودمند جلوه دهند.

۹-۳ آشنایی با مفهوم ویروس رایانه‌ای

ویروس رایانه‌ای به برنامه‌های مخرب کوچکی گفته می‌شود که مخفیانه وارد رایانه می‌شوند و بدون اطلاع و اختیار کاربر خود را تکثیر می‌کنند. پس هر برنامه مخرب ، ویروس نیست. در واقع ویروس رایانه‌ای نوعی برنامه‌مخرب است که خواص زیر را داشته باشد :

- **بسیار کوچک و کم حجم باشد**
- **بدون اطلاع کاربر بر روی رایانه او منتقل شود**
- **بدون اطلاع کاربر تکثیر شده و به رایانه‌های دیگر منتقل شود**

ویروس رایانه‌ای

ویروس رایانه‌ای به برنامه‌های مخرب کوچکی گفته می‌شود که مخفیانه وارد رایانه می‌شوند و بدون اطلاع کاربر خود را تکثیر می‌کنند.

نام ویروس به این علت روی اینگونه از برنامه‌ها گذاشته شده است که عملکردی مشابهٔ ویروس‌های بیولوژیک دارند. یک ویروس بیولوژیک از طرق مختلفی ممکن است وارد بدن انسان شود و ممکن است تا مدّت زیادی به فعالیت مخفیانه در بدن بپردازد و پس از مدتی علائم وجود ویروس مشخص شود. یک ویروس رایانه‌ای نیز از طرق مختلفی ممکن است وارد رایانه شود و تا مدتها به فعالیت خود ادامه دهد و پس از مدتی اختلالاتی را در رایانه ایجاد نماید. ویروس‌های رایانه‌ای می‌توانند به اطلاعات و برنامه‌های موجود در رایانه آسیب رسانده و آنها را از بین ببرند.

ویروس‌های رایانه‌ای توسط برنامه‌نویسان مجرب برای آسیب رساندن به شرکتهای رقیب نرم‌افزاری، مختل کردن شبکه‌های رایانه‌ای یا سایر مقاصد مشابه نوشته می‌شوند و همراه برنامه‌های قفل‌شکسته، برنامه‌های رایگان، از طریق اینترنت و غیره به رایانه‌های دیگر انتقال می‌یابند.

۹-۴ انواع ویروس از نظر محل تاثیر گذاری

ویروس‌ها مثل سایر برنامه‌های رایانه‌ای نیاز به محلی برای ذخیرهٔ خود دارند، با این تفاوت که ویروسها محلی را انتخاب می‌کنند که برای رسیدن به اهداف شوم خود نزدیکتر و در دسترس تر باشند.
محل‌هایی که برای جایگیری ویروس‌ها محبوبیت بیشتری دارند بشرح زیر می‌باشند :

- **فایلهای اجرایی**
- **فایلهای غیر اجرایی**
- **رکورد راه انداز (Boot Record)**
- **جدول پارتیشن (Partition Table یا Master Boot Record)**

در ادامه با انواع ویروسها از نظر محل تاثیر گذاری بیشتر آشنا خواهیم شد :

۹-۴-۱ ویروسهای تاثیرگذار بر روی فایلهای اجرایی

اکثر ویروس‌ها بطور انگل وار به فایلهای اجرایی می چسبند و آنها را آلوده می‌کنند تا پس از اجرا شدن آنها فعال شده و ضمن تکثیر خود، اطلاعات را از بین ببرند. به همین منظور اغلب نرم افزارهای ضد ویروس، فایلهای اجرایی یا انشعاب های زیر را بررسی یا پاکسازی می کنند :

.SCR ، .DLL ، .OVL ، .BIN ، .SYS ، .COM ، .EXE

بنابراین فایلهای اجرایی با انشعاب های فوق از اصلی‌ترین محل های جایگیری ویروسها می‌باشند.

۹-۴-۲ ویروسهای تاثیرگذار بر روی فایلهای غیر اجرایی

بندرت ویروسها در فایل های غیر اجرایی مثل فایل های متنی یا بانکهای اطلاعاتی جای می‌گیرند. از ویروسهای تاثیرگذار بر روی فایل‌های غیر اجرایی می‌توان به ویروسهایی اشاره کرد که در انتهای اسناد **Word** یا **Excel** خود را پنهان می‌کنند. این ویروسها بصورت دستورات نرم‌افزارهای **Word** یا **Excel** هستند که پس از باز شدن سند به صورت خودکار اجرا می‌شوند.

معمولاً آثار مخرب ویروسها بر روی فایلهای غیر اجرایی نمایان می‌شود و کمتر مشاهده شده است که ویروسها ، خود را در فایل‌های غیر اجرایی پنهان کنند.

۹-۴-۳ ویروسهای تاثیرگذار بر روی رکورد راه‌انداز (Boot Record)

برخی دیگر از ویروس ها علاقهٔ خاصی به پنهان شدن در رکورد راه‌انداز دارند زیرا رکورد راه انداز، واحد راه‌اندازی سیستم عامل است که در سکتور شمارهٔ صفر دیسک‌سخت یا فلاپی‌دیسک قرار دارد و اینگونه از ویروسها با قرار گرفتن در این محل به محض روشن شدن رایانه و اجرای یک برنامه آلوده به ویروس و یا دسترسی به رکورد راه انداز ، همراه آن در حافظهٔ اصلی جا می گیرند و بعضی از آنها تا موقع خاموش شدن رایانه همانجا باقی مانده و فایلهای دیگر را آلوده می کنند. حتی اگر برنامهٔ آلوده را حذف کرده یا فلاپی دیسک آلوده را نیز از دیسک گردان بیرون آورید.

رکورد راه‌انداز : Boot Record

اولین سکتور یک دیسک است که در این سکتور توضیحاتی در مورد دیسک از قبیل تعداد سکتورهای دیسک ، تعداد کلاستر‌ها و ... قرار دارد علاوه بر این اطلاعات ، در دیسک‌های راه‌انداز این سکتور شامل برنامه‌ای است که سیستم عامل را در حافظه قرار داده و آن را راه‌اندازی می‌کند.

۹-۴-۴ ویروسهای تاثیرگذار بر روی جدول Partition

عملکرد ویروسهای تاثیرگذار بر روی جدول **Partition** همانند ویروسهای تاثیر گذار بر روی رکورد راه‌انداز هستند. این ویروس‌ها علاقه خاصی به پنهان شدن در جدول **Partition** دارند زیرا جدول **Partition** شامل اطلاعات تقسیم بندی دیسک سخت است که در سکتور شمارهٔ صفر دیسک سخت قرار دارد. اینگونه از ویروسها با قرار گرفتن در این محل به محض روشن شدن رایانه و اجرای یک برنامه آلوده به ویروس و یا دسترسی به جدول **Partition** آلوده، همراه آن نرم‌افزار در حافظهٔ اصلی جا می‌گیرند و گاهی اوقات تا موقع خاموش شدن رایانه همانجا باقی مانده و فایلهای دیگر را آلوده می‌کنند. همچنین ویروس‌هایی یافت می شوند که اطلاعات مربوط به **Setup** سیستم را نیز خراب کرده یا تغییر می‌دهند.

۹-۵ روشهای انتقال ویروس

ویروس‌های رایانه‌ای ممکن است از راه‌های زیر به رایانه انتقال یابند :

۹-۵-۱ انتقال ویروس از طریق دیسکت یا سی‌دی آلوده

بعضی از ویروس‌ها با چسبیدن به انتهای فایل‌های اجرایی (با پسوند **EXE** و **COM**) یا با قرار گرفتن روی سکتور دیسکت خود را به روی رایانه منتقل می‌کنند.

با اجرای فایل‌های آلوده یا با قرار دادن دیسکت آلوده در رایانه و استفاده از آن، ویروس به رایانه منتقل شده و فعالیت خود را آغاز می‌کند.

۹-۵-۲ انتقال ویروس از طریق شبکه

هرگاه یکی از رایانه‌های متصل به شبکه آلوده به ویروس باشد، ممکن است ویروس از طریق شبکه همهٔ رایانه‌ها را آلوده نماید. بعضی از ویروس‌ها مخصوص شبکه هستند و ابتدا رایانه سرویس دهنده (**Server**) را آلوده می‌کنند و سپس توسط رایانه سرویس‌دهنده، کلیه رایانه‌های شبکه را آلوده می‌سازند.

۹-۵-۳ انتقال ویروس از طریق اینترنت

با گسترش استفاده از اینترنت، ویروس‌های اینترنتی به عنوان نسل جدیدی از ویروس‌ها مطرح شدند. ویروس‌های اینترنتی بسیار سریعتر از ویروس‌های دیگر در سطح دنیا انتشار می‌یابند، به صورتیکه ظرف چند روز میلیونها رایانه در سراسر دنیا به یک ویروس جدید آلوده می‌شوند. این نوع ویروس‌ها ممکن است از طریق پست الکترونیک و یا از طریق دریافت فایل از اینترنت و ... به رایانه منتقل شوند.

۹-۶ اصول تشخیص ویروسی شدن سیستم

ارائه روش دقیق و مشخصی برای تشخیص ویروسی بودن رایانه امکان پذیر نیست اما از آنجاییکه همهٔ ویروس‌ها درصدد ایجاد مزاحمت و اختلال در کار رایانه هستند و عملکرد همهٔ آنها منفی می‌باشد، لذا می‌توان از روی عملکرد آنها و عوارض ناشی از عملکرد آنها، ویروسی‌شدن سیستم را تشخیص داد. عملکرد ویروسها را که در واقع راههایی برای تشخیص ویروسی‌شدن سیستم می باشند می‌توان بشرح زیر دسته بندی کرد :

- **ایجاد تاخیر، وقفه یا اختلال در عملیات راه اندازی رایانه یا اجرای برنامه‌ها و فایلهای اجرایی.**

- **تخریب یا حذف اطلاعات و برنامه‌ها و یا حتی فرمت کردن دیسکها.**

- **اشغال حافظه و تکثیر در حافظه بطوریکه جایی برای اجرای برنامه های دیگر وجود نداشته باشد.**

مزاحمت‌ها و اختلال‌های فوق ممکن است به محض فعال شدن ویروس انجام شوند.

بطور کلی علائم زیر می‌تواند نشان‌دهنده ویروسی شدن رایانه باشد :

۹-۶-۱ کند شدن سیستم

البته هر نوع کند شدن سیستم را نمی‌توان به ویروسها مرتبط کرد. کند شدن سیستم ممکن است به علت اجرای برنامه‌های متعدد، کم بودن حافظه اصلی رایانه ، پایین بودن مشخصات رایانه و ... باشد. ولی اگر رایانه شما قبلاً با همین وضعیت سرعت مناسبی داشته و هم‌اکنون سرعت اجرای برنامه‌ها کم شده ، ممکن است سیستم شما ویروسی شده باشد.

۹-۶-۲ اشکال در راه‌اندازی سیستم

اگر هنگام راه‌اندازی رایانه ، مشکلی پیش آید و رایانه راه‌اندازی نشود، ممکن است رایانه ویروسی شده باشد. معمولاً این ویروسها بر روی سکتور صفر دیسک سخت قرار می‌گیرند. بعضی از این ویروسها هنگام راه‌اندازی سیستم پیغامی را نمایش می‌دهند و به کاربر اعلام می‌کنند که رایانه ویروسی است. یکی از این ویروسها ، ویروس **One Half** است که در هنگام راه‌اندازی رایانه، عبارت زیر را نمایش می‌دهد :

This is One Half ...

۹-۶-۳ اشکال در اجرای فایلهای اجرایی

اگر فایل‌های اجرایی رایانه، دچار مشکل شوند و اجرا نشوند ممکن است این فایل‌ها به ویروس آلوده شده باشند. گاهی اوقات وقتی یک فایل اجرایی به ویروس آلوده می‌شود، اندکی اندازه آن افزایش پیدا می‌کند. ولی ویروسهایی هم هستند که بدون آنکه اندازه یک فایل را تغییر دهند ، آن را آلوده می‌کنند.

۹-۶-۴ کند شدن ارتباط با اینترنت

بعضی از ویروسها ، اطلاعات رایانه ما را بصورت مخفیانه از طریق اینترنت به نویسنده ویروس ارسال می‌کنند. بعضی از ویروسها ممکن است از طریق اینترنت خود را تکثیر کنند. یعنی پس از متصل شدن رایانه به اینترنت شروع به تکثیر خود در اینترنت نمایند. بنابراین کند شدن ارتباط با اینترنت نیز می‌تواند یکی از دلایل ویروسی شدن رایانه باشد.

۹-۷ روشهای مقابله با ویروسها

در علوم پزشکی معروف است که پیشگیری آسانتر از درمان است در خصوص ویروسهای رایانه‌ای نیز همین جمله کاملاً مصداق دارد، بطور کلی راههای اصلی مقابله و مبارزه با ویروسها به دو دستهٔ زیر تقسیم می شوند :

- شناسائی ویروس ها و جلوگیری از ورود آنها به رایانه (پیشگیری).
- از بین بردن ویروس های وارد شده به رایانه و در صورت لزوم به وضعیت عادی بر گرداندن وضعیت سیستم (درمان).

بعضی از راههای مقابله با ویروسی شدن سیستم عبارتند از :

- ویروس‌ها هنگام ورود به سیستم به ناچار باید روی حافظه، برنامه و یا ناحیهٔ سیستمی دیسک قرار گیرند لذا معمولاً در سیستم یک حالت نوشتن اطلاعات بوجود می آید که این عمل تا حدودی قابل کنترل است. مثلاً با Write Protected کردن فلاپی دیسک یا در صورت امکان Write Protected کردن فلش دیسک [illegible]
- حتی‌المقدور از اتصال به رایانه‌ها و شبکه‌هایی که از عدم ویروسی بودن آنها اطمینان ندارید بپرهیزید. [illegible]
- هرگز از فلش دیسک‌ها یا CD هایی که از عدم ویروسی بودن آنها اطمینان ندارید استفاده نکنید. امروزه بسیاری از ویروس‌ها از خاصیت Autorun فلش دیسک‌ها برای تکثیر خود استفاده می‌کنند و با قرار دادن فلش دیسک در رایانه بلافاصله Autorun اجرا شده و باعث آلوده شدن رایانه می‌شود. [illegible]
- روی سیستم خود حتماً برنامه های ضد ویروسی که قابلیت مقیم شدن در حافظه را دارند قرار دهید. [illegible]
- تنظیمات مربوط به کنترل ویروس را در Setup سیستم خود انجام دهید. [illegible]
- وقتی ویروسی بر روی ناحیهٔ سیستمی دیسک یا بر روی فایل برنامه می نشیند، اندازه، تاریخ یا بعضی دیگر از مشخصات فایل اجرایی را تغییر می دهد. لذا می توان با تهیهٔ Backup های مرتب و مقایسه مشخصات فایلهای اجرایی و برنامه‌ها با نسخه‌های قبلی آنها از وجود احتمالی ویروس آگاهی پیدا کرد. [illegible]

۹-۸ روشهای مقابله با ویروسهای اینترنتی

با گسترش شبکه اینترنت ، ویروسها راه مناسب و سریعتری را برای گسترش و تکثیر خود پیدا کردند بصورتی که اکثر ویروسهای امروزی از طریق اینترنت منتقل می‌شوند

ویروس اینترنتی

ویروس‌های اینترنتی به آن دسته از ویروس‌های رایانه‌ای اطلاق می‌شود که از طریق اینترنت تکثیر یافته و منتقل می‌شوند.

ویروس‌های اینترنتی اغلب از طرق زیر وارد رایانه می‌شوند:

- **انتقال از طریق نامه‌های الکترونیکی (E-mail)**

به همراه نامه‌های الکترونیکی می‌توان فایل‌هایی را به صورت ضمیمه ارسال نمود. این فایل‌های ضمیمه ممکن است حاوی ویروس باشند. متأسفانه نامه‌های الکترونیکی بدون ضمیمه نیز می‌توانند حاوی ویروس باشند. به علت ضعف‌های امنیتی نرم‌افزارهای دریافت نامه‌های الکترونیکی نظیر نرم‌افزار **Outlook Express** ممکن است نامه‌های بدون ضمیمه نیز مخرب باشند. از معروفترین و خطرناکترین ویروس‌های اینترنتی که از طریق نامه‌های الکترونیکی انتقال می‌یابد، می‌توان به ویروس **NIMDA** اشاره کرد. این ویروس در عرض چند روز میلیونها رایانه را در سراسر دنیا آلوده کرد و متأسفانه هنوز هم مواردی از آلودگی به این ویروس مشاهده می‌شود.

- **انتقال از طریق دریافت فایل آلوده از اینترنت**

ممکن است در صفحات وب فوق متن دریافت فایلهای اجرایی وجود داشته باشد. که با کلیک کردن این فوق‌متن‌ها، یک فایل اجرایی و یا یک سند از طریق اینترنت دریافت شود. این فایلها ممکن است به ویروس‌ها آلوده باشند. در اینترنت سایتهایی وجود دارد که نرم‌افزارهای قفل شکسته را به صورت رایگان در اختیار افراد قرار می‌دهند. ممکن است این نرم‌افزارها آلوده به ویروس باشد.

بهترین راه مبارزه با ویروس‌های اینترنتی، پیشگیری از آلوده شدن به اینگونه ویروس‌هاست. برای جلوگیری از آلوده شدن به ویروسهای اینترنتی به توصیه‌های ساده اما مهم زیر توجه کنید :

- نامه‌های الکترونیکی مشکوک را باز نکنید.
- ضمیمه‌های نامه‌های الکترونیکی ناشناس را باز نکنید.
- اگر ضمیمه نامه‌ها، فایلهای اجرایی یا اسناد نرم‌افزارهایی نظیر Microsoft Word بود بدون بررسی توسط نرم‌افزارهای ضد ویروس آنها را اجرا نکنید.
- فایل‌ها و برنامه‌هایی که از اینترنت دریافت می‌کنید، حتماً با نرم‌افزارهای ضد ویروس بررسی کرده و پس از اطمینان از سالم بودن فایل‌های دریافتی ، از آنها استفاده نمایید.
- نرم‌افزارهای ضد ویروس خود را به موقع بروز رسانی نمایید.
- سیستم‌عامل و نرم‌افزارهای اینترنتی خود را به موقع بروز رسانی نمایید.
- همواره از اخبار ویروس‌های جدید مطلع باشید. سایتهای مفیدی در این زمینه وجود دارند که آخرین اطلاعات ویروس‌های جدید را برای شما ارسال می‌کنند. این اطلاعات که به صورت نامه الکترونیکی برای شما ارسال می‌شود، حاوی اطلاعاتی در مورد نحوه شناسایی ویروس و فعالیتهای که ویروس انجام می‌دهد و نحوه حذف آن است. تعدادی از این سایتها عبارتند از:

http://www.ca.com/us/anti-virus.aspx
http://housecallpro.trendmicro.com/housecall/default.asp

۹-۹ آشنایی با مراحل پاکسازی سیستم آلوده

درصورتیکه به هر دلیلی رایانه ما به ویروس آلوده شد ، باید هر چه سریعتر برای پاکسازی آن اقدام کنیم. برای پاکسازی ویروسها نمی‌توان یک روش مشخص را تعیین کرد زیرا هر ویروس عملکرد خاصی دارد که با توجه به نحوه تاثیرگذاری ویروس ، نوع ویروس ، نحوه آلوده کردن سیستم و ... باید روش مناسبی را برای پاکسازی ویروس انتخاب کرد. ما در این قسمت پاکسازی ویروسها را به سه روش کلی توضیح می‌دهیم که هر روش برای پاکسازی ویروسهای خاصی کاربرد دارد.

۹-۹-۱ پاکسازی ویروسهای مقیم در حافظه

ویروسهای مقیم در حافظه، اغلب ویروسهایی هستند که بر روی رکورد راه‌انداز یا جدول **Partition** قرار دارند و در هنگام راه‌اندازی رایانه فعال شده و در حافظه باقی می‌مانند. تا هنگامی که این ویروسها در حافظه قرار دارند، نمی‌توان برای پاکسازی آنها اقدام نمود.

برای پاکسازی این نوع ویروسها مراحل زیر را انجام می‌دهیم :

- *در صورت روشن بودن رایانه، آن را مجدداً راه‌اندازی می‌نماییم.*
- *رایانه را با یک دیسکت یا **CD** راه‌انداز سالم و عاری از ویروس ، راه‌اندازی می‌کنیم.*
- *دیسکت یا **CD** ضد ویروس مناسب را در درایو قرار داده و ویروسها را پاکسازی می‌نماییم.*
- *درصورتیکه سیستم عامل رایانه آسیب دیده است و یا سیستم راه‌اندازی نمی‌شود می‌باید با توجه به نوع سیستم عامل ، عملیات بازسازی و احیاء سیستم عامل انجام شود.*

۹-۹-۲ پاکسازی ویروسهای غیر مقیم در حافظه

از آنجایی که این ویروسها در حافظه فعال نیستند، کافیست با نرم‌افزار ضدویروس مناسب آنها را پاکسازی نماییم.

برای پاکسازی این نوع ویروسها مراحل زیر را انجام می‌دهیم :

- *دیسکت یا **CD** ویروس یاب مناسب را در درایو قرار داده و ویروسها را پاکسازی می‌نماییم.*

۹-۹-۳ پاکسازی ویروسهای اینترنتی

همانطور که می‌دانیم ویروسهای اینترنتی ، از طریق اینترنت به رایانه منتقل می‌شوند. پس هنگام پاکسازی این ویروسها باید اتصال به اینترنت را قطع نمود زیرا ممکن است بلافاصله پس از پاکسازی ویروس، رایانه مجدداً آلوده شود.

برای پاکسازی این نوع ویروسها مراحل زیر را انجام می‌دهیم :

- *ارتباط با اینترنت را قطع می‌کنیم.*
- *با توجه به دستورالعمل پاکسازی ویروس ، ممکن است نیاز باشد رایانه را مجدداً راه‌اندازی می‌کنیم.*
- *دیسکت یا **CD** ضد ویروس مناسب را در درایو قرار داده و ویروسها را پاکسازی می‌نماییم.*

۹-۱۰ آشنایی با نرم‌افزارهای ضدویروس

یکی از روشهای جلوگیری از انتقال ویروس به رایانه و حذف ویروسها از رایانه استفاده از نرم‌افزارهای ضد ویروس است. نرم‌افزارهای ضد ویروس نرم‌افزارهایی هستند که فایلهای آلوده به ویروس را شناسایی کرده و ویروس را از روی رایانه حذف می‌کنند.

همان طوری که می‌دانید همه روزه ویروس های جدید با ساختار و عملکردهای مختلف توسط ویروس نویسان ساخته می شوند که شناسایی ساختار و عملکرد آنها و تهیهٔ برنامه‌های ضد ویروس مناسب آنها، مستلزم صرف هزینه و وقت نسبتاً زیادی است. به همین دلیل تهیهٔ ضد ویروس مناسب هر ویروس، براحتی امکان پذیر نیست و هیچ شرکت تولید کنندهٔ برنامه های ضد ویروس، نمی تواند ادعا نماید که قادر به شناسائی و از بین بردن تمام ویروس‌ها می باشند و تا زمانیکه ضد ویروس یک ویروس جدید طراحی می گردد ممکن است رایانه‌های زیادی آلوده و دچار اختلال گردند.

از معروفترین و متداولترین نرم‌افزارهای ضد ویروس می‌توان به نرم‌افزارهای زیر اشاره کرد:

- **AVG Antivirus**
- **Avira Antivirus**
- **Bit Defender Antivirus**
- **Dr. Web**
- **ESET NOD32 Antivirus**
- **Kaspersky Virus Remove Tool**
- **McAfee Virus Scan**
- **Norton Antivirus**
- **Panda Antivirus**
- **Rising Antivirus**

اکثر نرم‌افزارهای ضد ویروس فقط می‌توانند ویروسهای شناخته شده را تشخیص دهند و قادر نیستند ویروسهای جدید را تشخیص دهند. برای حل این مشکل ، در نرم‌افزارهای ضد ویروس امکان بروزرسانی در نظر گرفته شده است به صورتیکه از طریق اینترنت می‌توان نرم‌افزار ضد ویروس را بروزرسانی کرد. شرکتهای تولید کننده نرم‌افزارهای ضد ویروس، جدیدترین ویروسها را شناسایی کرده و فایل‌های بروزرسانی نرم‌افزار ضد ویروس خود را در وب سایت قرار می‌دهند تا مشترکین آنها در سراسر دنیا نرم‌افزارهای خود را بروزرسانی نمایند.

۹-۱۰-۱ روشهای مقابله نرم‌افزارهای ضدویروس با ویروسها

نرم‌افزارهای ضد ویروس به روش‌های زیر با ویروسها مقابله می‌کنند :

- **پیشگیری از آلوده شدن به ویروس**

در هنگام وارد شدن ویروس به رایانه ، پیغام هشدار دهنده‌ای را به کاربر نمایش می‌دهند و از فعال شدن ویروس خودداری می‌کنند.

- **پاک کردن ویروس**

فایلهای سالمی که به ویروس آلوده شده اند را شناسایی می‌کنند و در صورت امکان آنها را ویروس‌زدایی کرده و به صورت اولیه باز می‌گردانند به این عمل **disinfecting** (ویروس‌زدایی) می‌گویند.

- **قرنطینه کردن فایل ویروسی**

درصورتیکه نتوانند یک فایل‌آلوده را ویروس‌زدایی کنند آن فایل را قرنطینه کرده و به کاربر اطلاع می‌دهند که این فایل آلوده به ویروس است و امکان ویروس زدایی آن نیست و فعلاً در قرنطینه است. درصورتیکه کاربر مایل باشد می‌تواند این فایل را به کلی حذف کند. همچنین نرم‌افزارهای ضد ویروس به کاربران اجازه می‌دهند، فایل‌های مشکوک را به قسمت قرنطینه منتقل کنند.

۹-۱۱ آشنایی با نرم‌افزار Norton Antivirus

این نرم‌افزار توسط شرکت **Symantec** طراحی شده است. از مهمترین مزایای این ضدویروس، به روزرسانی ساده و سریع آن از طریق اتصال به اینترنت است. در این کتاب ، از نسخه ۲۰۰۹ نرم‌افزار **Norton Antivirus** استفاده شده است.

۹-۱۱-۱ نصب نرم‌افزار Norton Antivirus

برای نصب نرم‌افزار Norton Antivirus عملیات زیر را انجام می‌دهیم :

*CD نصب نرم‌افزار **Norton Antivirus** را در درایو قرار داده و فایل **NAVSetup.exe** را اجرا می‌کنیم.*

شکل (۹-۱) اجرای برنامه نصب Norton Antivirus

پنجره خوش‌آمد گویی نصب، مطابق شکل (۹-۲) ظاهر می‌شود. دکمه AGREE & INSTALL *را برای ادامه نصب کلیک می‌کنیم.*

شکل (۳-۹) پنجره خوش‌آمدگویی نصب Norton Antivirus 2009

- در پنجره بعدی عملیات کپی فایل‌های نرم‌افزار *Norton Antivirus* انجام می‌شود.
- بعد از انجام عملیات نصب، پنجره شکل (۳-۹) ظاهر می‌شود. در این پنجره توضیحاتی در مورد نحوه خرید نرم افزار نمایش داده شده است. در قسمت پایین پنجره بر روی عبارت ***buy later*** کلیک می‌کنیم و خرید نرم افزار را به آینده موکول می‌کنیم. (حداکثر ۱۵روز می‌توان به صورت رایگان از نرم افزار استفاده کرد و پس از آن باید خرید انجام شود)

شکل (۳-۹) پنجره خرید نرم افزار

- در پنجره بعد، دکمه DONE را برای پایان عملیات نصب کلیک می‌کنیم.

شکل (۴-۹) پنجره پایانی نصب

- در پایان پنجره اصلی نرم افزار **Norton Antivirus** مطابق شکل (۵-۹) ظاهر می‌شود و آیکن نرم‌افزار نیز در ناحیه سینی ویندوز (**System Tray**) قرار می‌گیرد.

شکل (۵-۹) پنجره اصلی نرم افزار **Norton Antivirus**

۹-۱۱-۲ شناسایی و پاکسازی ویروسها با نرم‌افزار Norton Antivirus

نرم‌افزار **Norton Antivirus** پس از نصب، بصورت مقیم در حافظه قرار می‌گیرد. در ضمن هربار که رایانه را روشن کنیم این نرم‌افزار به صورت خودکار اجرا شده و در حافظه قرار می‌گیرد. هر فایل یا پوشه‌ای را که باز کنیم، نرم‌افزار **Norton** بصورت خودکار فایل‌های داخل آن را پوشه را بررسی می‌کند و درصورتیکه فایل ویروسی پیدا کند بلافاصله پیغامی را نمایش می‌دهد و از فعالیت ویروس جلوگیری می‌کند.

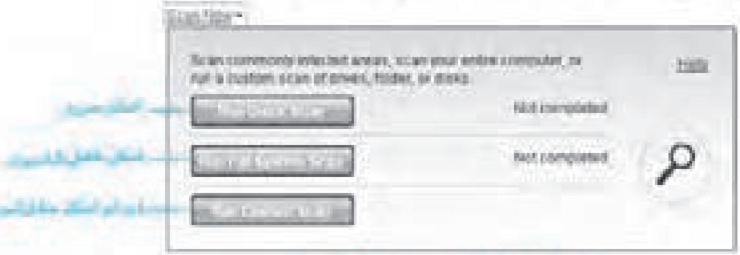
گاهی اوقات ممکن است بخواهیم تمام یا بخشی از فایل‌های رایانه را ویروس‌یابی کنیم.

برای ویروس‌یابی رایانه عملیات زیر را انجام می‌دهیم :

- *بر روی آیکن در سینی نوار کار، کلیک می‌کنیم.*

شکل (۹-۴) آیکن نرم‌افزار ضد ویروس Norton

- *پنجره اصلی نرم‌افزار **Norton Antivirus** مطابق شکل (۹-۵) ظاهر می‌شود. برای ویروس‌یابی بر روی کلیک می‌کنیم.*
- *منویی مطابق **Error! Reference source not found.** ظاهر می‌شود.*



شکل (۹-۶) منوی انتخاب نوع Scan

در این پنجره دکمه‌های زیر وجود دارد :

- 

با کلیک روی این دکمه، فقط فایل‌هایی که معمولاً مورد حمله ویروس‌ها قرار می‌گیرند بررسی می‌شود. برخی از فایل‌هایی که مورد بررسی قرار می‌گیرند عبارتند از : فایل‌های مهم پوشه ویندوز، رجیستری ویندوز ، پوشه **My Documents** و برخی از فایل‌های درایوی که سیستم عامل ویندوز بر روی آن نصب شده است. این روش اسکن بسیار سریعتر از روش **Full System Scan** است.

- Run Full System Scan

با کلیک روی این دکمه، کلیه فایل‌های موجود در رایانه ویروس‌یابی می‌شود.

- Run Custom Scan

با کلیک روی این دکمه ، می‌توان انتخاب کرد که کدام درایو یا کدام پوشه یا حتی کدام فایل مورد بررسی قرار گیرد.

پس از کلیک کردن این دکمه، پنجره شکل (۸-۹) ظاهر می‌شود.

شکل ۸-۹ پنجره Scans نورتن

در این پنجره می‌توان بر اساس نیاز خود یکی از گزینه‌های زیر را انتخاب کرد :

- Full System Scan

با کلیک روی این دکمه، کلیه فایل‌های موجود در رایانه ویروس‌یابی می‌شود.

- Scan drives

با کلیک روی این دکمه ، پنجره‌ای باز می‌شود که می‌توان درایو یا درایوهای مورد نظر برای ویروس‌یابی را انتخاب نمود.

شکل ۹-۹ پنجره انتخاب درایوها برای ویروس‌یابی

- Scan folders

با کلیک بر روی این دکمه ، پنجره‌ای باز می‌شود که می‌توان پوشه یا پوشه‌های مورد نظر برای ویروس‌یابی را انتخاب نمود.

شکل ۹-۱۰ پنجره انتخاب پوشه‌ها برای ویروس‌یابی

- Scan files

با دوبار کلیک بر روی این دکمه ، پنجره‌ای باز می‌شود که می‌توان فایل یا فایل‌های مورد نظر برای ویروس‌یابی را انتخاب نمود.

شکل ۹-۱۱ پنجره انتخاب فایل‌ها برای ویروس‌یابی

پس از انتخاب هر یک از موارد فوق ، پنجره‌ای مطابق شکل (۹-۱۲) ظاهر می‌شود و کلیه فایل‌ها، پوشه‌ها یا درایوهایی که مشخص کرده‌ایم را ویروس‌یابی می‌کند.

شکل ۹-۱۲ پنجره ویروس‌یابی فایل‌ها و پوشه‌های تعیین شده

- در پایان عملیات ویروس‌یابی ، پنجره‌ای مطابق شکل (۱۳-۹) ظاهر می‌شود.

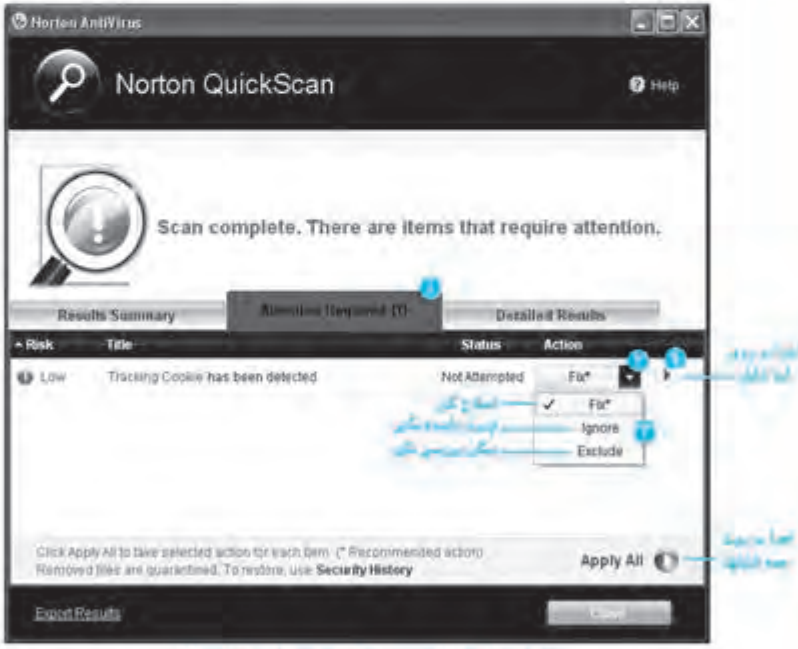
شکل (۱۳-۹) پنجره نمایش نتیجه عملیات ویروس‌یابی

- نرم افزار **Norton** به صورت پیش فرض هر فایل ویروسی که پیدا کند ، ویروس را از داخل فایل حذف می‌کند. اگر نرم افزار **Norton** فایل ویروسی یا تهدید امنیتی را پیدا کند که نتواند آن را رفع کند، این خطرات را در سربرگ **Attention Required** نمایش می‌دهد و از ما می‌خواهد که نحوه حذف ویروس یا رفع خطر امنیتی را مشخص کنیم.
- بر روی سربرگ **Attention Required** کلیک می‌کنیم. لیستی از فایل‌های ویروسی نمایش داده می‌شود.
- در ستون **Action** ، عملیات پیشنهادی برای هر فایل ویروسی ، نمایش داده شده است. برای تغییر عملیات پیشنهاد شده ، در این ستون بر روی هر آیتم کلیک می‌کنیم تا لیستی از عملیات‌های ممکن نمایش داده شود. در کنار یکی از گزینه‌ها علامت * دیده می‌شود که به معنی عملیات پیشنهادی نرم افزار **Norton** است. (لیستی از گزینه‌هایی که ممکن است پیشنهاد شود و عملکرد هر یک در جدول (۱-۹) نمایش داده شده است.)

گزینه	عملیات
Fix	عملیات لازم برای بر طرف کردن خطر را انجام می‌دهد.
Ignore	هیچ عملیاتی انجام نمی‌دهد ولی در دفعات بعدی باز هم این فایل به عنوان ویروس شناخته خواهد شد.
Exclude	هیچ عملیاتی انجام نمی‌دهد ولی در دفعات بعد این فایل ویروس‌یابی می‌شود.
Get Help	شما را به قسمت راهنمایی وب سایت **Symantec** متصل می‌کند تا دستورالعمل حذف این ویروس را مشاهده کنید.
Rescan	مجددا فایل را مورد ویروس یابی قرار می‌دهد.

جدول (۱-۹) گزینه‌های پیشنهادی برای رفع خطر ویروس

- گزینه مورد نظر را از لیست انتخاب کرده و دکمه ▶ را برای رفع خطر کلیک می‌کنیم. یا دکمه Apply All را برای رفع همه خطرات موجود در لیست کلیک می‌کنیم.



شکل (۱-۹) سربرگ Attention Required

- در سربرگ ***Detailed Results*** جزییات نتایج حاصل از ویروس یابی و حذف ویروس‌ها نمایش داده می‌شود.

شکل (۱۵-۹) پنجره Detailed Results

۹-۱۱-۳ تنظیمات نرم افزار Norton Antivirus

نرم افزار ضد ویروس **Norton** ، تنظیمات مختلفی را در اختیار کاربر قرار می‌دهد تا کاربر بتواند تغییرات مورد نظر خود را در نحوه **Scan** کردن ، ظاهر نرم افزار و ... در نرم افزار اعمال کند.

برای اعمال تغییرات مورد نظر در نرم افزار **Norton Antivirus** مراحل زیر را انجام می‌دهیم :

- در پنجره اصلی نرم‌افزار ***Norton Antivirus*** بر روی Settings کلیک می‌کنیم.
- پنجره ***Settings*** مطابق شکل (۱۶-۹) ظاهر می‌شود. در این پنجره تنظیمات مختلفی در چهار گروه وجود دارد. اکثر تنظیمات بصورت On و Off است که با هر بار کلیک بر روی آن تغییر می‌کند.
- در این پنجره تغییرات مورد نظر را انجام داده و دکمه OK را کلیک می‌کنیم.

همانطور که در شکل (۱۶-۹) مشاهده می‌شود ، در پنجره **Settings** ، چهار گروه تنظیمات وجود دارد :

- تنظیمات رایانه (Computer Settings)

در این قسمت می‌توان تنظیمات امنیتی ، تنظیمات مربوط به **Scan** کردن و تنظیمات بروزرسانی را انجام داد.

- تنظیمات اینترنت (Internet Settings)

در این قسمت می‌توان تنظیمات مربوط به امنیت مرورگر ، تنظیمات مربوط به بررسی پست‌الکترونیک و تنظیمات مربوط به نرم‌افزارهای پیام رسان اینترنتی را انجام داد.

- **تنظیمات شبکه خانگی (Home Network Settings)**

در صورت اتصال به شبکه خانگی ، تنظیمات امنیتی مربوط به شبکه در این قسمت انجام می‌شود.

- **تنظیمات متفرقه (Miscellaneous Settings)**

تنظیمات ظاهری نرم افزار و تنظیمات متفرقه دیگر در این قسمت قرار دارد.

شکل (۹/۱۶) پنجره Settings

۹-۱۱-۲ Norton Insight

یکی از مشکلات استفاده از نرم‌افزارهای ضد ویروس ، کند شدن رایانه است زیرا نرم افزار ضد ویروس ، تمامی فایل‌هایی که در حال خوانده شدن یا اجرا شدن هستند را به صورت خودکار مورد بررسی قرار می‌دهد و پس از اینکه از سالم بودن آنها مطمئن شد ، اجازه خوانده شدن یا اجرا شدن را می‌دهد و این موضوع باعث پایین آمدن کارایی رایانه می‌شود.

یکی از امکانات نرم افزار ضد ویروس **Norton** ، ابزار **Norton Insight** است. این ابزار به صورت خودکار فایل‌ها و برنامه‌هایی که بسیار مورد استفاده قرار می‌گیرند و سالم بودن آنها محرز است را شناسایی کرده و از این به بعد نرم افزار ضد ویروس آنها را بررسی نمی‌کند و با این روش کارایی رایانه بالا می‌رود.

برای اجرا کردن و استفاده از ابزار **Norton Insight** عملیات زیر را انجام می‌دهیم :

- بر روی آیکن در سینی نوار کار، کلیک می‌کنیم.
- پنجره اصلی نرم‌افزار **Norton Antivirus** مطابق شکل (۵-۹) ظاهر می‌شود. بر روی Norton Insight کلیک می‌کنیم.
- پنجره **Norton Insight** ظاهر می‌شود. در این پنجره لیستی از پردازش‌ها و فایل‌هایی که هم‌اکنون اجرا شده اند نمایش داده می‌شود. در ستون **Rating** نمره اطمینانی که نرم افزار **Norton** به هر فایل می‌دهد نمایش داده می‌شود. فایل‌هایی که ۵ ستاره هستند یعنی از نظر نرم‌افزار ضد ویروس **Norton** ، مورد اطمینان هستند.
- پس از بررسی همه فایل‌ها، نرم افزار **Norton Insight** فایل‌های مورد اطمینان را شناسایی کرده و در ستون **Trust Level** ، عبارت **Norton Trust** را برای فایل‌های مورد اطمینان نمایش می‌دهد. از این پس این فایل‌ها توسط ضد ویروس **Norton** مورد بررسی قرار نمی‌گیرند و در نتیجه سرعت و کارایی رایانه نسبت به قبل افزایش می‌یابد.
- دکمه Close را برای بستن این پنجره کلیک می‌کنیم.

شکل ۲۱-۹ پنجره Norton Insight

۹-۱۱-۵ غیر فعال کردن نرم افزار Norton Antivirus

نرم افزارهای ضد ویروس معمولا در ابتدای راه‌اندازی ویندوز به صورت خودکار شروع به کار کرده و در هنگام **Shutdown** کردن ویندوز ، از حافظه خارج می‌شوند. ولی گاهی اوقات ممکن است بخواهیم به صورت موقت نرم افزار ضد ویروس را غیر فعال کنیم. به عنوان مثال می‌خواهیم نرم افزاری را نصب کنیم که از لحاظ وظایف با نرم افزار ضد ویروس تداخل کاری دارد (مثلا نصب نرم افزار ضد ویروس دیگری یا نصب نرم افزار **Firewall** یا ...)

برای غیر فعال کردن نرم افزار Norton Antivirus عملیات زیر را انجام می دهیم :

- بر روی آیکن در سینی نوار کار، راست کلیک می‌کنیم.
- در منوی ظاهر شده ، گزینه *Disable Antivirus Auto-Protect* را کلیک می‌کنیم.

شکل ۱۸-۹ منوی ظاهر شده پس از راست کلیک روی آیکن نرم افزار Norton Antivirus

- پنجره‌ای مطابق شکل (۱۹-۹) ظاهر می‌شود. در این پنجره مدت زمانی که می‌خواهیم نرم افزار ضد ویروس غیرفعال باشد را از لیست *Select Duration* انتخاب کرده و دکمه OK را کلیک می‌کنیم.

شکل ۱۹-۹ پنجره Security Request

۹-۱۱-۶ بروزرسانی نرم‌افزار Norton Antivirus

همانطور که اشاره کردیم ، ممکن است ظرف یک هفته یا چند روز ویروسهای جدیدی توسط افراد خرابکار تولید شود. نرم‌افزارهای ضدویروس فقط قادر به شناسایی ویروسهای شناخته شده هستند بنابراین نیاز است که هر چند روز یکبار آنها را بروزرسانی نماییم. شرکتهای تولید کننده نرم‌افزارهای ضد ویروس، آخرین ویروسها را در سطح دنیا شناسایی می‌کنند و پس از تشخیص عملکرد و نحوه پاک کردن آنها، اطلاعات ویروس و نحوه حذف آن را در سایتهای اینترنتی خود قرار می‌دهند. در ضمن امکان بروزرسانی نرم‌افزارهای ضد ویروس را از طریق اینترنت به کاربران خود می‌دهند.

برای بروزرسانی نرم‌افزار **Norton Antivirus** عملیات زیر را انجام می‌دهیم :

- *ابتدا به اینترنت متصل می‌شویم.*
- *بر روی آیکن در سینی نوار کار، کلیک می‌کنیم.*
- *پنجره اصلی نرم‌افزار **Norton Antivirus** مطابق شکل (۵-۹) ظاهر می‌شود. برای ویروس‌یابی بر روی کلیک می‌کنیم.*
- *برنامه **Live Update** به اینترنت متصل شده و اطلاعات شناسایی و حذف ویروسهای جدید را دریافت می‌کند.*

شکل (۲۰-۹) پنجره Live Update

۹-۱۲ خواندن و درک متون انگلیسی

متن انگلیسی زیر را خوانده و به سئوالات پاسخ دهید.

Security risks, such as spyware and adware, can compromise your personal information and privacy. Spyware and adware programs are closely related. In some cases, their functionalities may overlap, but while they both collect information about you, the types of information that they collect can differ.

Spyware programs may put you at risk for identity theft or fraud. These programs can log your keystrokes and capture your email traffic and instant messaging traffic. These programs can also steal sensitive personal information such as passwords, login IDs, or credit card numbers. These programs can then send your compromised data to other people.

Adware displays advertisements on your computer and collects information about your Web browsing habits. It then gives this data to companies that can send you the advertisements that are based on these preferences.

Tracking cookies are the small files that programs can place on your computer to track your computing activities. Tracking cookies can then report that information back to a third party.

Some programs rely on other programs that are classified as security risks to function. For example, a shareware or freeware program that you download may use adware to keep its price low.

۱) **Spyware** چیست؟ چه عملیاتی بر روی رایانه انجام می‌دهد؟ شرح دهید.

۲) **Adware** چیست؟ شرح دهید.

۳) **Spyware** و **Adware** چه شباهتها و چه تفاوتهایی دارند؟

۴) نرم‌افزارهای **Shareware** و **Freeware** چه مشکلات امنیتی ممکن است داشته باشند؟

۵) **Cookie** ها چه نوع برنامه‌هایی هستند؟ چه خطر امنیتی ممکن است داشته باشند؟

تمرین

۱ - از طریق اینترنت به سایت **http://www.antivirus.com** متصل شوید و اطلاعاتی در مورد ویروس‌های جدید اینترنتی بدست آورید.

۲ - به آدرس **http://www.imenantivirus.com/encyclChm/encyclChm** متصل شوید. در این سایت اطلاعاتی در مورد ویروس‌های اینترنتی به زبان فارسی وجود دارد. مشخصات و نحوه عملکرد چند ویروس را بدست آورید.

۳ - نرم‌افزار **Norton Antivirus** را بر روی رایانه خود نصب نمایید.

۴ - رایانه خود را **Quick Scan** کنید سپس یکبار دیگر **Full Scan** نمایید. چه تفاوتی بین این دو نوع ویروس‌یابی وجود دارد؟

۵ - درایو C رایانه را ویروس‌یابی نمایید.

۶ - فقط پوشه ویندوز را ویروس‌یابی نمایید.

۷ - فقط فایل **Calc.exe** در پوشه **Windows\system32** را ویروس‌یابی نمایید.

۸ - نرم افزار ضدویروس را برای یک ساعت غیر فعال کنید.

۹ - با اجرای **Norton Insight** کارایی رایانه را بالا ببرید.

۱۰ - از طریق اینترنت نرم‌افزار **Norton Antivirus** را بروزرسانی نمایید.

آزمون تشریحی

۱ - برنامه‌های مخرب را تعریف نمایید وانواع آن را نام ببرید.

۲ - ویروس رایانه‌ای را تعریف نمایید.

۳ - خواص ویروسهای رایانه‌ای را نام ببرید.

۴ - انواع ویروس از نظر محل تاثیر گذاری را نام برده و عملکرد آنها را شرح دهید.

۵ - روش‌های انتقال ویروس به رایانه را نام ببرید.

۶ - راههای تشخیص ویروسی شدن سیستم را نام ببرید.

۷ - علائم ویروسی شدن سیستم را نام ببرید.

۸ - ویروس اینترنتی را شرح دهید.

۹ - روش‌های انتشار ویروس‌های اینترنتی را نام ببرید.

۱۰ - روشهای مقابله با ویروس‌های اینترنتی را شرح دهید.

۱۱ - نرم‌افزار ضد ویروس را تعریف کرده و چند نمونه از آنها را نام ببرید.

۱۲ - روش‌های مقابله نرم‌افزارهای ضد ویروس با ویروس‌ها را شرح دهید.

۱۳ - علت بروزرسانی نرم‌افزارهای ضدویروس چیست؟

آزمون چهارگزینه‌ای

۱ - کدام گزینه از انواع برنامه‌های مخرب نیست؟

الف) Worm **ب)** Trojan **ج)** Freeware **د)** Bomb

۲ - کدامیک جزئی ویروس را بیان نیست؟

الف) بسیار کوچک و کم حجم است.

ب) بدون اطلاع کاربر بر روی رایانه او منتقل می‌شود.

ج) با قراردادن دیسک‌ها در کنار هم منتقل می‌شود.

د) بدون اطلاع کاربر تکثیر شده و به رایانه‌های دیگر منتقل می‌شود

۳ - انتقال ..... از روش‌های انتقال ویروس می‌باشد.

الف) از طریق دیسک آلوده **ب)** از طریق CD آلوده

ج) از طریق شبکه و اینترنت **د)** هر سه گزینه

۴ - کدام یک از روش‌های انتقال ویروس را سریعتر منتشر می‌کند؟

الف) از طریق اینترنت **ب)** از طریق CD آلوده

ج) از طریق دیسک آلوده **د)** از طریق شبکه

۵ - کدامیک از علائم زیر نشانه ویروسی شدن سیستم است؟

الف) ایجاد تاخیر، وقفه یا اختلال در عملیات راه اندازی رایانه یا اجرای برنامه‌ها و فایلهای اجرایی.

ب) اشغال حافظه و تکثیر در حافظه بطوریکه جایی برای اجرای برنامه های دیگر وجود نداشته باشد.

ج) تخریب یا حذف اطلاعات و برنامه‌ها و یا حتی فرمت کردن دیسکها.

د) هر سه گزینه

۶ - ویروسهای ..... از طریق نامه‌های الکترونیکی وارد رایانه می‌شوند.

الف) اینترنتی **ب)** سیستمی

ج) مخرب **د)** مقیم در حافظه

۷ - برای جلوگیری از آلوده شدن به ویروسهای اینترنتی کدامیک از روش‌های زیر مؤثر است؟

الف) باز نکردن نامه‌های الکترونیکی مشکوک **ب)** بروزرسانی نرم‌افزار ضد ویروس

ج) بروزرسانی سیستم عامل **د)** هر سه مورد

۸ - روش‌های مقابله نرم‌افزارهای ضدویروس با ویروس‌ها ..... است.

الف) پیشگیری از آلوده شدن به ویروس **ب)** پاک کردن ویروس

ج) قرنطینه کردن فایل ویروسی **د)** هر سه مورد

۹ - درصورتیکه دیسکتی که احتمالا حاوی ویروس است به شما داده شده است و شما نیاز دارید که از این دیسکت استفاده نمایید برای اینکه رایانه شما ویروسی نشود چه کاری باید بکنید؟

الف) دیسکت را فرمت می‌کنیم.

ب) ابتدا دیسکت را ویروس‌یابی کرده و پس از حذف ویروس‌ها از آن استفاده می‌کنیم.

ج) ابتدا دیسکت را **Write Protect** کرده و پس از حذف ویروس‌ها از آن استفاده می‌کنیم.

د) گزینه‌های ب و ج

۱۰ - فرض کنید بر روی یک دیسکت چند فایل قرار داده‌اید و می‌خواهید این فایل‌ها را در رایانه دوست خود کپی کنید با توجه به اینکه رایانه دوست شما سمگی است ویروسی باشد چه کاری باید انجام دهید تا دیسکت شما ویروسی نشود؟

الف) دیسکت را فرمت می‌کنیم.

ب) دیسکت را از حالت **Write Protect** خارج کرده و سپس آن را در درایو رایانه قرار می‌دهیم.

ج) دیسکت را در حالت **Write Protect** قرار داده و سپس آن را در درایو رایانه قرار می‌دهیم.

د) هیچکدام

۱۱ - برای بروزرسانی نرم‌افزار **Norton Antivirus** از کدام دکمه استفاده می‌شود؟

الف) **Status** **ب)** **Online** **ج)** **Live Update** **د)** **Register**

۱۲ - در نرم‌افزار **Norton Antivirus** برای ویروس‌یابی یک فایل در درایو C بهتر است از کدام دکمه زیر استفاده شود؟

الف) Full System Scan **ب)** Scan folders **ج)** Scan drives **د)** Scan files

۱۳ - در کدام روش ویروس‌یابی فقط فایل‌هایی که بیشتر مورد حمله قرار می‌گیرند مورد بررسی قرار می‌گیرند؟

الف) **Full System Scan** **ب)** **Quick Scan** **ج)** **Sean Drives** **د)** **Sean Folders**

پاسخنامه آزمون چهارگزینه‌ای

فصل اول

سوال	الف	ب	ج	د	سوال	الف	ب	ج	د	سوال	الف	ب	ج	د
۱				✓	۲		✓			۳			✓	
۴			✓		۵		✓							

فصل دوم

سوال	الف	ب	ج	د	سوال	الف	ب	ج	د	سوال	الف	ب	ج	د
۱		✓			۲		✓			۳		✓		
۴			✓		۵	✓				۶				✓
۷		✓			۸		✓			۹				✓
۱۰			✓		۱۱			✓		۱۲	✓			
۱۳		✓			۱۴				✓					

فصل سوم

سوال	الف	ب	ج	د	سوال	الف	ب	ج	د	سوال	الف	ب	ج	د
۱	✓				۲			✓		۳				✓
۴				✓	۵	✓				۶				✓
۷		✓			۸			✓		۹			✓	
۱۰		✓			۱۱				✓	۱۲	✓			
۱۳		✓			۱۴		✓			۱۵				✓
۱۶		✓			۱۷		✓			۱۸	✓			
۱۹			✓		۲۰				✓	۲۱		✓		
۲۲	✓				۲۳			✓						

فصل چهارم

سوال	الف	ب	ج	د	سوال	الف	ب	ج	د	سوال	الف	ب	ج	د
۱			✓		۲	✓				۳		✓		
۴				✓	۵				✓	۶			✓	

فصل پنجم

سوال	الف	ب	ج	د	سوال	الف	ب	ج	د	سوال	الف	ب	ج	د
۱		✓			۲					۳			✓	
۴	✓				۵		✓			۶				✓
۷	✓				۸		✓			۹	✓			
۱۰		✓			۱۱			✓		۱۲				✓
۱۳				✓	۱۴		✓			۱۵				✓
۱۶			✓											

فصل ششم

سوال	الف	ب	ج	د	سوال	الف	ب	ج	د	سوال	الف	ب	ج	د
۱			✓		۲		✓			۳		✓		
۴		✓			۵		✓			۶			✓	

فصل هفتم

سوال	الف	ب	ج	د	سوال	الف	ب	ج	د	سوال	الف	ب	ج	د
۱			✓		۲			✓		۳			✓	
۴	✓				۵				✓	۶				✓
۷		✓			۸			✓		۹			✓	
۱۰		✓			۱۱		✓			۱۲				✓
۱۳		✓												

فصل هشتم

سوال	الف	ب	ج	د	سوال	الف	ب	ج	د	سوال	الف	ب	ج	د
۱	✓				۲	✓				۳		✓		
۴		✓			۵			✓		۶			✓	
۷		✓			۸				✓	۹		✓		
۱۰			✓		۱۱		✓			۱۲		✓		
۱۳			✓		۱۴			✓		۱۵				✓
۱۶				✓	۱۷			✓		۱۸				✓
۱۹		✓												

فصل نهم

سوال	الف	ب	ج	د	سوال	الف	ب	ج	د	سوال	الف	ب	ج	د
۱			✓		۲					۳			✓	
۴	✓				۵				✓	۶	✓			
۷				✓	۸				✓	۹		✓		
۱۰			✓		۱۱					۱۲				✓
۱۳		✓												

فهرست منابع

۱) مولفین گروه آموزش مهارت ، اطلاعات و ارتباطات - مهارت هفتم ICDL XP ، نشر صفار ، ۱۳۸۳

۲) مولفین گروه آموزش مهارت ، مفاهیم شبکه - رایانه کار درجه یک ، نشر صفار ، ۱۳۸۶

۳) فرهنگ واژه‌های مصوب فرهنگستان ۱۳۷۶ تا ۱۳۸۵، نشر آثار ، ۱۳۸۷

۴) فرهنگ واژه‌های مصوب فرهنگستان دفتر پنجم ، نشر آثار ، ۱۳۸۷

۵) منابع و مقالات اینترنتی معتبر ، ۲۰۰۹

6) Microsoft Computer Dictionary, fifth Edition, Microsoft Press, 2002

7) Stalling William, Data and Computer Communications, 8th Edition, Prentice Hall, 2007

8) Libor Dostalek and Alexa Kabelova, Understanding TCP/IP, PACKT Publishing, 2006