همه چیز درباره ویروس‌ها، کرم‌ها، اسب‌های تروا و فراتر از آن

« بخش سوم »

کلیه حقوق این مقاله متعلق به سایت امنیت وب و مترجم آن می باشد و هر گونه برداشت از آن فقط با ذکر نام سایت و نام نویسنده مجاز می باشد.

مترجم : رضا مددی / rzmadadi@yahoo.com

منبع : www.Sophos.com

تاریخ : 20 اردیبهشت ۱۳۸۳

در صورتی که شما :

- **یک مدیر شبکه هستید،**
- **فردی هستید که با دوستان خود دیسک مبادله می‌کند،**
- **از شبکه‌های محل کار خود استفاده می‌کنید،**
- **و یا فقط خواننده نامه‌های الکترونیکی هستید،**

بدانید که این مطلب برای شماست!

ما حقایق را در باره ویروس‌های کامپیوتری بطور ساده و با زبانی قابل فهم برای شما بیان می‌کنیم.

فهرست مطالب

بخش اول

- چرا ویروس‌ها مهم هستند؟
- ویروس ها، اسب‌های تروا و کرم‌ها
- تعریفی ساده از ویروس، اسب تروا، کرم
- ویروس چیست؟
- ویروس چگونه بر روی کامپیوتر تاثیر می‌گذارد؟
- اسب‌های تروا
- کرم‌ها
- ویروس‌ها چه کارهایی می‌توانند انجام دهند؟
- خطر مربوط به ویروس‌ها در چه جاهایی وجود دارد؟
- جلوگیری کردن از ویروس‌ها
- ویروس‌های سکتور بوت
- ویروس‌های انگلی
- ویروس‌های ماکرو (کلان دستور)

بخش دوم

- نرم‌افزار ضد ویروس
- پویشگرها
- Checksummer ها
- نرم‌افزارهای کاشف (Heuristic)
- هزینه‌های پنهانی ویروس‌ها
- ویروس‌نویسان چه کسانی هستند؟
- آیا نوشتن ویروس همیشه نادرست است؟
- ویروس‌های گول‌زن (Hoax ها)
- Hoax ها چیستند؟
- چرا Hoax ها یک معضل هستند؟
- چه کارهایی را در مورد Hoax ها می‌توان انجام داد؟
- تاریخچه مختصری از ویروس‌ها
- ۱۰ ویروس برتر

بخش سوم

- پست الکترونیک
- آیا به صرف خواندن نامه، ویروسی می‌شویم؟
- ویروس‌هایی که بطور خودکار از طریق نامه‌ها گسترش می‌یابند
- خطرات فایل‌های پیوندی
- چگونه ویروس‌های پستی را متوقف کنیم؟
- اینترنت
- کلیک کردن و آلوده شدن؟
- آیا به صرف دیدن وب‌سایت‌ها، ویروسی می‌شویم؟
- دستورات برنامه‌نویسی وب‌سایت‌ها
- اسب‌های تروای «در پشتی» و اینترنت
- آیا کوکی‌ها خطرناک هستند؟
- حمله‌ها به سوی وب‌سرورها
- امنیت در شبکه

بخش چهارم

- تلفن‌های موبایل و کامپیوترهای کف‌دستی
- آیا ویروس‌های موبایل هم وجود دارند؟
- تلفن‌های WAP و ویروس‌ها
- خطرات آتی برای WAP
- سیستم‌عامل‌های کامپیوترهای کف‌دستی
- ویروس‌ها برای یخچال‌ها؟
- چگونگی محافظت از ابزارهای متحرک (Mobile)
- ده مرحله برای ایجاد امنیت در کار با کامپیوتر
- لینک‌های مفید

بخش سوم

پست الکترونیک

در صورتیکه از افراد بخواهید فقط یک ویروس را برای شما نام ببرند، شانس ویروس‌های Melissa ، Love Bug ، Sobog ، I Love You و چند ویروس دیگر بیشتر از بقیه خواهد بود. علت آنکه این ویروس‌ها به چنین عمومیتی دست یافته و در تیترهای خبری جای گرفته‌اند آن است که آنها توانسته‌اند از طریق پست الکترونیک در سرتاسر جهان انتشار پیدا کنند.

در حال حاضر پست الکترونیک بزرگترین منشاء ویروس‌ها می‌باشد، چرا؟

تا زمانی که ویروس‌ها بوسیله دیسکت انتقال پیدا می‌کردند، انتشارشان بسیار کند بود. شرکت‌ها می‌توانستند استفاده از دیسکت‌ها را ممنوع کرده یا کاربران را مجبور به بررسی دیسکت‌ها برای حصول اطمینان از عدم وجود ویروس نمایند.

اما پست الکترونیک همه چیز را تغییر داده است. در حال حاضر شما می‌توانید فایل‌هایتان را با سرعتی بسیار بیشتر مبادله کنید و در عوض، دستگاه شما هم براحتی یک کلیک بر روی یک آیکون و شاید هم ساده‌تر از آن آلوده می‌شود. ویروس‌های معمولی این امکان را دارند که بسیار سریعتر از گذشته منتشر شده و انواع جدیدتر ویروس هم می‌توانند کارکرد برنامه‌های پست الکترونیک را مورد سوء استفاده خود قرار دهند.

آیا به صرف خواندن نامه، ویروسی می‌شویم؟

بعضی از کاربران فکر می‌کنند تا وقتی که به فایل‌های پیوندی نامه‌ها کاری نداشته باشند، باز کردن و خواندن نامه‌های اشکالی ندارد و آنها از امنیت کافی برخوردار خواهند بود. در حال حاضر چنین تفکری دیگر ارزشی ندارد.

ویروس‌هایی مانند Kakworm و Bubbleboy می‌توانند کاربران را در هنگامی که فقط نامه‌هایشان را می‌خوانند آلوده کنند. آنها شبیه سایر نامه‌ها هستند با این تفاوت که شامل یک اسکریپت مخفی می‌باشند. این اسکریپت مخفی به محض باز کردن نامه یا مشاهده آن در صفحه پیش‌نمایش (Preview Pan) – در صورتیکه شما از برنامه Outlook به همراه نسخه منطبقی از Internet Explorer استفاده کنید – اجرا خواهد شد. اسکریپت

مـورد نظـر می‌تواند تنظیمات سیستم را تغییر داده و ویروس را از طریق پست الکترونیک برای سایر کاربران ارسال کند.

شـرکت مایکروسافت فایل ترمیمی مورد نیاز برای از بین بردن این ضعف امنیتی را منتشر کرده است. برای دریافت آن می‌توانید به آدرس زیر مراجعه کنید :

www.microsoft.com/technet/security/bulletin/ms99-032.asp

ویروس‌های Hoax پست الکترونیک

پست الکترونیک رسانه‌ای محبوب برای **Hoax** ها می‌باشد.

Hoax ها گزارش‌هایی دروغین از ویروس‌ها می‌باشند که از شما درخواست می‌کنند تا آنها (گزارش‌ها) را برای تمام افرادی که می‌شناسید ارسال کنید.

یـک **Hoax** پسـت الکترونـیک مـی‌تواند مانند ویروس در شبکه‌ها انتشار پیدا کرده و باعث ایجاد بار ترافیکی عظیمی از نامه‌ها شود. تفاوت در آنجاست که **Hoax** مانند ویروس نیازی بـه کدنویسی ندارد و گسترش آن فقط به خوش باوری کاربران بستگی دارد. برای اطلاعات بیشتر به قسمت «ویروس‌های گول‌زن (**Hoax** ها)» از بخش دوم مراجعه کنید.

ویروس‌هایی که بطور خودکار از طریق نامه‌ها گسترش می‌یابند.

امروزه اکثرا ویروس‌های موفق آنهایی هستند که خود را بصورت خودکار از طریق پست الکترونیک منتشر می‌کنند.

نوعـا کارکرد این ویروس‌ها به کلیک کردن کاربر بر روی فایل پیوندی نامه بستگی دارد. در اینصـورت اسـکریپتی اجـرا خواهـد شـد کـه با استفاده از برنامه مربوط به پست الکترونیک، اسناد آلوده را برای سایر کاربران پست الکترونیک ارسال خواهد کرد.

بـرای مـثال ویـروس **Melissa** پـیغام را بـه پـنجاه آدرس اول از تمـام کـتابچه آدرس‌هایـی کـه در دسـترس بـرنامه **Microsoft Outlook** باشـند، ارسـال می‌کند. سایر ویروس‌ها خود را به تمام آدرس‌های کتابچه آدرس ارسال می‌کنند.

اسپم چیست؟

اسپم نامه‌ای ناخواسته است که محتوای آن اغلب تبلیغ طرح‌هایی ارزن و سریع، شغل‌های داخل منزل و وب‌سایت‌های اجاره‌ای و یا غیر مشروع می‌باشد. اسپم‌ها اکثرا اطلاعات بازگشتی جعلی در خود داشته و شناسایی ارسال کننده آن از روی نامه بسیار مشکل می‌باشد. چنین نامه‌هایی را فقط باید پاک کرد.

خطرات فایل‌های پیوندی

در حال حاضر بزرگترین خطر امنیتی، نه نامه‌های الکترونیک بلکه الصاقات آنها می‌باشد.

هر برنامه، سند یا فایل صفحه گسترده‌ای که از طریق نامه دریافت می‌کنید می‌تواند شامل ویروس باشد و اجرا کردن چنین فایلی می‌تواند کامپیوتر شما را آلوده سازد.

متاسفانه پیوند به نامه‌های الکترونیکی روشی محبوب برای تبادل اطلاعات می‌باشد. بسیاری از کاربران فکر می‌کنند گردش در بین Screen Saver ها، کارت‌های تبریک، تصاویر انیمیشن و یا برنامه‌های تفریحی، تفریحی بی‌خطر است در حالیکه چنین فایل‌هایی هم می‌توانند حامل ویروس باشند.

حتی یک فایل پیوندی که به نظر می‌رسد فایلی از نوع ایمن - مثلا فایلی با پسوند txt. - باشد، می‌تواند عاملی برای تهدید باشد. ممکن این فایل متنی در واقع یک اسکریپت مخرب ویژوال بیسیک با پسوند vbs. باشد که از دید پنهان شده است.

کرم VBS/Monopoly نمونه‌ای از یک برنامه مخرب می‌باشد که به صورت یک برنامه تفریحی تغییر قیافه داده است. این کرم وانمود می‌کند که برنامه‌ای تفریحی درباره بیل گیتس (Bill Gates) میباشد. همینگونه هم است (یک صفحه بازی به همراه تصاویر مایکروسافت را نمایش می‌دهد)، اما علاوه بر اینکار خود را مخفیانه برای کاربران دیگر هم ارسال کرده و جزییات سیستم شما را به آدرس‌های بخصوصی ارسال می‌کند که اینکار محرمانه بودن اطلاعات حساس شما را تهدید می‌کند.

دیدزدن و جعل نامه

دیـدزدن نامـه بـه این معناست که سایر کاربران بتوانند نامه شما که در حال گذر از مسـیر بـرای رسیدن به مقصد است را بخوانند. شما برای محافظت از نامه‌ها و جلوگیری از اینکار می‌توانید نامه‌هایتان را رمز کنید.

جعـل نامـه بـه معـنای فرستادن نامه با ثبت آدرسی جعلی از فرستنده یا قرار دادن نامه در نامه دیگران می‌باشد. شما برای تشخیص چنین نامه‌هایی باید از امضاهای دیجیتالی استفاده کنید.

چگونه ویروس‌های پستی را متوقف کنیم؟

داشتن سیاستی دقیق در قبال فایل‌های پیوندی نامه‌ها

تغیـیر رفـتار خـود یا سایر کاربران ساده‌ترین راه برای مقابله با تهدیدات نامه‌های الکترونیکـی مـی‌باشـد. هـیچ فـایل پیوندی حتی اگر از جانب بهترین دوستتان باشد را باز نکنـید. در صورتیکه از پاک بودن چیزی مطمئن نیستید، با آن مانند فایلی آلوده رفتار کنید. شـما باید سیاست مشخصی برای شرکت خود داشته و تمام فایل‌های پیوندی را قبل از اجرا توسط نرم‌افزارهای ضد ویروس بررسی کرده و صلاحیت آن‌ها را تایید کنید.

استفاده از نرم‌افزارهای ضد ویروس

از نـرم‌افـزار ضـد ویروس با خاصیت دسترسی فعال، هم در دروازه ورود و خروج نامه‌ها و هم بر روی کامپیوتر استفاده کنید. استفاده از این ترکیب می‌تواند شما را در مقابل ویروس‌هایی که از طریق نامه‌ها فرستاده می‌شوند، محافظت کند.

انواع ناخواسته فایل‌ها را در همان دروازه ورودی بلوکه کنید.

ویـروس‌ها اغلب از انواع فایلی VBS ، SHS ، EXE ، SCR ، CHM و BAT برای انتشـار خود استفاده می‌کنند. بعید است که سازمان شما همیشه به فایل‌هایی از این نوع که از خـارج سـازمان فرسـتاده می‌شوند، نیاز داشته باشد، بنابراین می‌توانید آنها را در همان دروازه ورود نامه‌ها بلوکه کنید.

در دروازه ورود، فایل‌های با پسوند مضاعف را بلوکه کنید

بعضـی ویـروس‌هـا برنامه بودن خود را با استفاده از «پسوند مضاعف» در بعد از نام خود مخفی می‌کنند مانند txt.vbs. . چنین فایل‌هایی را در دروازه ورود بلوکه کنید.

اینترنت

اینترنت اطلاعات بسیار زیادی را بسیار سریعتر از قبل، در اختیار بسیاری از مردم قرار می‌دهد. اما بخش دیگر این مساله آن است که اینترنت دسترسی کدهای مخرب کامپیوتری به کامپیوترهای شرکت‌ها و منازل را هم آسوده‌تر کرده است.

کلیک کردن و آلوده شدن؟

اینترنت خطر آلودگی را افزایش داده است.

ده سال قبل، بیشتر ویروس‌ها از طریق دیسکت‌ها گسترش می‌یافتند. انتشار ویروس با این روش کند بود و به میزان توجه کاربران به اجرای برنامه‌های جدید بستگی داشت. اگر هم ویروس تاثیرات جانبی بسیار مشهودی داشت، اما بعید بودکه بتواند کاربران خیلی زیادی را آلوده کند. در حال حاضر از آنجایی که شبکه اینترنت در مقیاس بسیار وسیعی مورد استفاده قرار می‌گیرد، همه چیز تغییر یافته است.

به اشتراک گذاشتن نرم‌افزار بر روی شبکه کار آسانی است. با یک کلیک ماوس می‌توان برنامه‌ای را به یک نامه پیوند زد و باز کردن و اجرای آن هم ساده می‌باشد. کاربران براحتی می‌توانند برنامه‌ها را بر روی صفحات وب قرار داده و سایرین هم می‌توانند براحتی آنها را دریافت کنند، بنابراین ویروس‌های فایلی (انگلی) می‌توانند از طریق برنامه‌های Download شده رونق زیادی در شبکه‌ها داشته باشند.

در این بین ویروس‌هایی که واقعا سود می‌برند، ویروس‌های ماکرو هستند که بر روی اسناد (متون) تاثیر می‌گذارند. کاربران به طور متناوب اسناد یا فایل‌های صفحه گسترده را از اینترنت دریافت کرده و یا آنها را از طریق پست الکترونیک مبادله می‌کنند. تمام آنچه که شما برای آلوده کردن کامپیوترتان باید انجام دهید آن است که بر روی یک فایل دریافت شده از اینترنت یا یک فایل پیوندی کلیک کنید.

هنگامی که از اینترنت استفاده می‌کنید، اسناد را با برنامه‌ای باز کنید که می‌تواند ماکروها را نادیده بگیرد، همچنین برنامه‌هایی که از منبع نامطمئنی دریافت شده‌اند را اجرا نکنید.

آیا به صرف دیدن وب‌سایت‌ها، ویروسی می‌شویم؟

دیـدن یک وب‌سایت کم‌خطرتر از باز کردن برنامه‌ها یا اسناد ناشناخته است. با این حـال ایـن کار هم خطر دارد. خطر مورد اشاره به انواع دستورات بکار برده شده در طراحی سـایت و اقدامـات امنیتـی در نظر گرفته شده توسط ISP شما و خود شما بستگی دارد. در بخش بعد انواع اصلی کدهایی که شما با آنها مواجه هستید آورده شده‌اند.

دستورات برنامه‌نویسی وب‌سایت‌ها

HTML

صفحات وب با زبان HTML (زبان نشانه‌گذاری فرامتن) نوشته می‌شوند. این زبان به نویسندگان وب اجازه می‌دهد تا متن‌هایشان را قالب‌بندی کرده و لینک‌هایی به تصاویر و یـا سـایر صـفحات ایجـاد کنند. کدهای HTML به خودی خود حامل ویروس نمی‌باشد، اما صـفحات وب مـی‌توانـند شـامل کدهایی باشند که بطور خودکار برنامه‌ها را اجرا کرده و یا اسناد را باز می‌کنند. این کار خطر اجرای یک فایل آلوده را به همراه دارد.

ActiveX

ActiveX یکـی از تکـنولوژی‌هـای شـرکت مایکروسافت برای توسعه دهندگان وب بـوده و فقـط بـر روی کامپـیوترهای مبتنـی بـر سیسـتم عامل ویندوز مورد استفاده قرار می‌گیرد.

اپلـت‌هـای اکتـیوایکس کـه بـرای ایجـاد جلـوه‌های بصری در صفحه‌های وب مورد اسـتفاده قـرار مـی‌گـیرند، دسترسـی کامل به منابع سیستم کامپیوتر شما داشته و این کار مـی‌توانـد آنهـا را به تهدیدی بالقوه برای شما تبدیل کند. با این حال امضاهای دیجیتالی که مـی‌توانـند مجـاز و غـیر تحمیلـی بودن اپلتی را اثبات کنند، این قابلیت را دارند که امنیتی محدود را تامین نمایند.

Java

گاهـی اوقـات افـراد بـی‌جهـت دربـاره ویـروس‌هـای جاوا در شبکه اینترنت نگران مـی‌شـوند. ایـن امر به خاطر آن است که آنها اپلت‌های جاوا – که برای ساخت افکت بر روی صـفحه‌هـای وب مـورد اسـتفاده قرار می‌گیرد – را با برنامه‌ها و اسکریپت‌های جاوا اشتباه می‌گیرند.

Applet هـا عمومـا ایمـن می‌باشند. آنها توسط مرورگر در یک محیط امن که با نام sandbox (جعـبه شـن) شـناخته مـی‌شود، اجرا می‌شوند. حتی اگر وجود یک رخنه امنیتی

باعث گریز اپلتی شود باز هم یک اپلت مخرب نمی‌تواند براحتی انتشار پیدا کند. اپلت‌ها معمولا از یک سرور به کامپیوتر کاربران جریان دارند و نه از کامپیوتر یک کاربر به کامپیوتر کاربر دیگر (برای امتحان این مساله می‌توانید از دوستانتان بخواهید که از یک صفحه وب که دارای اپلت جاوا می‌باشد دیدن کنند، سپس یک کپی از اپلت را هم برای آنها ارسال کنید). علاوه بر مطالب فوق باید به این مساله اشاره کرد که اپلت‌ها به غیر از حافظه Cache مربوط به وب، در جایی از دیسک سخت ذخیره نمی‌شوند.

در صورتیکه با اپلتی آسیب آور مواجه شدید که بسیار شبیه به اسب تروا عمل می‌کرد، بدانید که در دستگاه خود حداقل یک برنامه مخرب دارید که خود را برای شما موجه و قانونی جلوه داده است.

Application های جاوا بطور واضح برنامه‌هایی هستند که در زبان Java نوشته می‌شوند. همانند تمام برنامه‌های دیگر آنها هم می‌توانند حامل ویروس باشند، بنابراین شما باید با همان احتیاطی که با برنامه‌های دیگر رفتار می‌کنید با این برنامه‌ها هم رفتار کنید.

Script جاوا اسکریپتی است که در داخل دستورات HTML بکار رفته شده در صفحات وب گنجانده شده است. مانند تمام اسکریپتهای دیگر، اسکریپتهای جاوا هم می‌توانند بطور خودکار دستورات خطرناکی را اجرا کنند. شما می‌توانید برای محافظت از خود اسکریپتهای فعال را غیر فعال کنید (به قسمت « امنیت در شبکه » در انتهای همین بخش مراجعه کنید.).

اسکریپتهای ویژوال بیسیک (VBS : Visual Basic Script)

اسکریپتهای ویژوال بیسیک بسته به مرورگر مورد استفاده می‌توانند به محض مشاهده شدن صفحه‌ای اجرا شوند. برای اجرای آنها نیازی به انجام کاری از سوی شما نیست. این نوع از اسکریپت‌ها توسط بعضی از انواع کرمهای پست الکترونیک مانند Kakworm و Bubbleboy مورد استفاده قرار گرفته‌اند، اما می‌توانند به همان خوبی و فقط با دیدن صفحه‌های وب هم اجرا شوند.

اسب‌های تروای «در پشتی» و اینترنت

اسب تروای «در پشتی» برنامه‌ای است که امکان در اختیار گرفتن کنترل کامپیوترهای کاربران از طریق اینترنت را برای افرادی فراهم می‌کند.

همانند اسب‌های تروای دیگر، اسب تروای «در پشتی» هم خود را به عنوان نرم‌افزاری موجه و دلخواه وانمود می‌کند. هنگامی که این برنامه اجرا می‌شود (معمولا بر روی سیستم‌های مبتنی بر سیستم‌عامل‌های ویندوز 95 و 98) خود را به لیست برنامه‌های

Startup کامپیوتر اضافه می‌کند. بعد از اجرا، این اسب تروا بر فعالیت‌ها و اطلاعات کامپیوتر نظارت دارد تا زمانی که ارتباطی با اینترنت برقرار شود. به هنگام on line شدن کامپیوتر، شخص فرستنده اسب تروا می‌تواند از نرم‌افزارهای دستگاه خود برای باز و بسته کردن برنامه‌های کامپیوتر آلوده، تغییر دادن فایل‌ها و یا حتی در اختیار گرفتن چاپگر آن استفاده کند. Sub7 و BackOrifice در بین بهترین اسب‌های تروای «در پشتی» شناخته شده قرار دارند.

آیا کوکی‌ها خطرناک هستند؟

کوکی‌ها بطور مستقیم تهدیدی برای کامپیوتر شما یا اطلاعات آن نمی‌باشند. با این حال آنها می‌توانند محرمانه بودن اطلاعات شما را تهدید کنند چرا که :

کوکی، وب سایت مربوط به خود را قادر می‌سازد تا جزییات کارهای شما را به خاطر بسپارد و سایت را در جریان مشاهدات شما قرار دهد. در صورتیکه شما دوست دارید تا ناشناس باشید، باید تنظیمات امنیتی مرورگرتان را در جهت غیر فعال کردن کوکیها میزان کنید.

حمله‌ها به سوی وب‌سرورها

تنها کاربران شخصی کامپیوترها در معرض خطر بر روی شبکه اینترنت نمی‌باشند. بعضی از هکرها وب‌سرورها - که باعث موجودیت وب‌سایت‌ها می‌شوند - را مورد هدف قرار داده‌اند.

شکلی معمولی از حمله به این صورت است که درخواست‌های بسیار زیادی را به وب‌سرور مورد نظر ارسال می‌کنند تا بر اثر پردازش آنها سرعت سرور افت پیدا کرده و یا اینکه بطور کل از کار بیفتد. هنگامی که این اتفاق رخ دهد، کاربران اصلی سایت که توسط سایت میزبانی می‌شدند دیگر به وب‌سایت‌های آن سرور دسترسی نخواهند داشت.

از نقاط ضعف دیگر، اسکریپت‌های CGI (Common Gateway Interface) می‌باشند. این اسکریپت‌ها برای اجرا و مدیریت موتورهای جستجو، دریافت اطلاعات از فرم‌ها و کارهایی مانند این بر روی وب‌سرورها اجرا می‌شوند. هکرها می‌توانند از اسکریپت‌هایی از نوع CGI که برنامه‌ریزی ضعیفی داشته‌اند برای در اختیار گرفتن کنترل یک سرور استفاده کنند.

امنیت در شبکه

در صورتیکه می‌خواهید بصورتی امن از شبکه اینترنت استفاده کنید، باید کارهای زیر را انجام دهید.

داشتن شبکه‌ای جداگانه برای کامپیوترهای مرتبط با اینترنت

شبکه‌های جداگانه‌ای را برای کامپیوترهای متصل به شبکه اینترنت و کامپیوترهایی که به شبکه متصل نیستند، تهیه کنید. این کار باعث کاهش خطر انتشار ویروس‌های فایل‌های آلوده دریافتی از اینترنت توسط کاربران، بر روی شبکه اصلی شما می‌شود.

استفاده از فایروال‌ها و(یا) مسیریاب‌ها

فایروال فقط اجازه داخل شدن اطلاعات مجاز به سازمان شما را صادر می‌کند.

مسیریاب هم مسیر بسته‌های اطلاعاتی دریافت شده از شبکه اینترنت را کنترل می‌کند.

تنظیم پیکربندی مرورگر وب برای بدست آوردن امنیت لازم

اپلت‌های جاوا و اکتیوایکس، کوکیها و ... را غیر فعال کرده و یا اینکه تنظیمات را طوری انجام دهید که به هنگام اجرای چنین کدهایی، شما هم باخبر شوید. برای مثال در برنامه Internet Explorer شرکت مایکروسافت، قسمت Custom Level از بخش Security مربوط به گزینه Internet Option از منوی Tools را انتخاب کرده و تنظیمات امنیتی مورد نظر را انجام دهید.