آشنائی با ویروسهای

کامپیوتری

فهرست

کرم های اینترنتی زمان کامپیوتر را تلف می کنند یا به عبارت دیگر آن را کند می کنند و همچنین در شبکه یا در اینترنت پهنای باند را اشغال می کنند. آنها تکثیر می شوند و اغلب اوقات نقش یک شیطان اینترنتی را بازی می کنند کرمی که Code Red نام دارد در سال ۲۰۰۱ صدر اخبار اینترنتی را به خود اختصاص داده بود. متخصصین پیش بینی کرده بودند که این کرم می تواند اینترنت را تا حد از کار افتادن کند سازد.

Code Redزمانیکه خود را تکثیر می کند سرعت اینترنت را کاهش می دهد. اما این کرم اینترنتی انگونه که پیش بینی می شد نتوانست اینترنت را متوقف سازد. هر کپی از این کرم در اینترنت بدنبال ویندوز سرور NT یا ۲۰۰۰ ای می گردد که در آن وصله های امنیتی مایکروسافت نصب نشده باشد .هر بار که یک سرور اینترنتی حفاظت نشده پیدا کند خود را در آن سرور کپی می کند. و کپی جدید بدنبال سرور دیگری با این شرایط می گردد تا آن را آلوده کند بسته به تعداد سرور های غیر ایمن Code Red می تواند در اینترنت صدها یا هزارها کپی از خود تهیه کند.

ویروس Code Red طوری طراحی شده است که سه کار انجام دهد.

- خود را برای بیست روز اول هر ماه تکثیر می کند .
- صفحات وبی را که در سرور های آلوده هستند را با صفحاتی که در آن نوشته شده است "Hacked by Chi nese"جایگزین می کند .
- سپس شروع به تدارک یک حمله علیه وب سایت کاخ سفید می کند تا آنرا از کار بیندازد

معمول ترین ورژن Cod Red یک نوع توسعه یافته از I da Code Red است که خود را در ۱۹ ژولای سال ۲۰۰۱ میلادی تکثیر کرد.

بعد ازیک آلوده ساختن موفقیت آمیز کرم منتظر یک ساعت مشخص می ماند و به دومین مورد نظر سرور کاخ سفید متصل می شود این حمله به این صورت است که سیستم های آلوده به طور همزمان ۱۰۰ ارتباط با پورت ۸۰ سایت (www.whi t ehouse.gov با I P:۱۹۸.۱۳۷.۲۴۰.۹۱) بر قرار می کند.

دولت امریکا آدرس I P وب سایت www.whi t ehouse.or g را تغییر داده است تا این حملات را خنثی کند و یک هشدار عمومی در مورد این کرم منتشر کرده است تا سرورهای وبی را که از ویندوز ۲۰۰۰ و NT استفاده می کنند از وجود و نحوه مبارزه با آن آگاه کند.

ویروسهای بوت سکتور

با گذشت زمان همانطور که ویروس نویسان ماهرتر و خبره تر شدند حقه های جدیدتری یاد گرفتند یک حقه که دانستن آن مهم است توانایی فراخوانی ویروس در حافظه است به طوریکه تا زمانیکه کامپیوتر کار می کند این ویروس ها جولان می دهند. که این خود باعث می شود که ویروسها خود را به بسیار راحتر تکثیر کنند یک حقه دیگر آلوده ساختن Boot Sector در فلاپی دیسک و هارد دیسک است Boot Sector .یک برنامهٔ کوچک است و اولین قسمت از سیستم عامل است که توسط کامپیوتر فراخوانی می شود Boot Sector .شامل یک برنامه کوچک است که برای کامپیوتر تعیین می کند که چگونه سیستم عامل را فراخوانی کند. یک ویروس با قرار دادن کد خود در Boot Sector اجرای خود را گارانتی می کند .بنابراین ویروس می تواند به راحتی در کامپیوتر فراخوانی شود بنابراین قادر است هر زمان که کامپیوتر روشن می شود شروع به کار کند. این ویروسها به راحتی می توانند بوت سکتور یک فلاپی دیسک را آلوده کنند و با انتقال آن بین کامپیوترهای دیگر مانند آتش ناشی از انفجار منتشر شوند.

اما امروزه این ویروسها مانند گذشته یک کابوس نیستند .چون امروزه گرافیک یک عنصر جدا نشدنی از نرم افزارها شده است و در نتیجه حجم آنها به شدت افزایش پیدا کرده است و به ندرت می توانید نرم افزاری را پیدا کنید که روی یک یا حتی چند فلاپی دیسک جا شود .امروزه نرم افزار ها بیشتر روی CD بین کامپیوتر ها جابجا می شوند و چون CD ها عموماً قابل رایت مجدد نیستند و اگر هم باشند باید بوسیله نرم افزار انجام شود این ویروسها و دیگر ویروسهای قابل اجرا به راحتی نمی توانند بین کامپیوتر ها تکثیر شوند. ولی هنوز اینترنت وجود دارد. پس همیشه خطر آلوده شدن وجود دارد.

SSLچیست؟

Secure socket LayerیاSSL پرتکلی است که بوسیله Netscape برای انتقال پرونده های خصوصی روی اینترنت بوجود آمده است SSL .توسط یک کلید شخصی کار می کند، تا اطلاعات انتقالی در اینترنت را برای شما پنهان کند. هر دو مرورگر اینترنت اکسپلورر و نت اسکیپ از SSL پشتیبانی می کنند. و بسیاری از سایتهای از این پروتکل استفاده می کنند، تا از اطلاعات محرمانه کاربران (مانند اطلاعات کارت اعتباری) نگهداری کنند.

آدرس سایتهایی که نیاز به SSL دارند باید به صورت https به جای http باشد. یک پرتکل دیگر برای انتقال مطمئن اطلاعات روی شبکه جهانی وب secure http یا s-http است. به طوریکه SSL یک ارتباط مطمئن بین یک کاربر و سرور ایجاد می کند. و هر اطلاعاتی را می توان با آن منتقل کرد. ولی s-http طراحی شده است تا پیام های شخصی را به طور ایمن انتقال دهد. بنابراین SSL و s-http را می توان به عنوان مکمل یکدیگر در نظر

گرفت، تا رقیب یکدیگر. هر دو پرتکل بوسیله) IETF که مخفف Internet Engineering Task Force است (به عنوان استاندارد تصویب شده است.

یک مشکل امنیتی معمول در ویندوز

متأسفانه بسیاری از کاربران ویندوز از یک شکاف امنیتی موجود در تنظیمات شبکه کامپیوتر بی اطلاع هستند.

تنظیمات معمول شبکه در ویندوز به شرح زیر است:

Client for Microsoft Networks

file and printer sharing for Microsoft Networks

NET BEUI Protocol

Internet Protocol TCP/IP

اگر در تنظیمات ویندوز شما **NetBIOS** مجاز باشد یک مشکل امنیتی در **TCP/IP** دارید.

- ممکن است فایلهای شما در کل اینترنت به اشتراک گذاشته شوند بدون انکه شما مایل به این عمل باشید.
- **Work Group-name , Computer name , Logn- name**برای دیگران قابل مشاهده است.
- فایلهای شما می‌توانند در کل اینترنت به اشتراک گذاشته شود.

کامپیوترهایی که به هیچ شبکه‌ای متصل نشده‌اند هم می‌توانند در معرض خطر باشند زمانیکه برای اولین بار به اینترنت متصل می‌شوید تنظیمات شبکه شما تغییر می‌کند.

حل مشکل:

برای کاربران ویندز ۲۰۰:

با disable کردن **NetBIOS** در **TCP/IP** می توانید مشکل را حل کنید:

- ویندوز اکسپیلورر را باز کنید.
- روی **My Network places** راست کلیک کنید.
- **properties**را انتخاب کنید.
- روی **Locol Are a Network** راست کلیک کنید.

- روی **properties** کلیک کنید.
- وارد قسمت **Bindings** شوید.
- علامت تیک **Clinet for Microsoft Network** را بردارید. علامت تیک **File and printer sharing**را بردارید.
- روی **OK** کلیک کنید.

اگر پیغامی مانند **"You must select a driver..."** :را دریافت کردید. روی **YES** کلیک کنید. و روی **OK** کلیک کنید تا پنجره های دیگر را ببندید.

اگر هنوز می خواهید فایلها و پرینتر شما در شبکه فعال باشد، باید از پروتکل **NetBEUI** به جای **TCP/IP** استفاده کنید. مطمئن باشید که آن را برای شبکه محلی خود فعال کرده اید.

مراحل به شرح زیر است:

- ویندوز اکسپیلورر را باز کنید.
- روی **My Network places** راست کلیک کنید.
- **properties**را انتخاب کنید.
- **NetBEUI**را انتخاب کنید.
- روی **properties** کلیک کنید.
- وارد قسمت **Bindings** شوید.
- برای **Clinet for Microsoft NetworkS** علامت تیک بگذارید.
- برای **File and printer sharing** علامت تیک بگذارید و روی OK کلیک کنید.

اکنون باید کامپیوتر خود را ری استارت کنید (restart) کنید. تا تغییرات در سیستم شما اعمال شوند.

دسترسی به اینترنت یک ریسک امنیتی است.

زمانی که به اینترنت دسترسی دارید. از یک آدرس IP مانند ۸۳ 150.61.130.برای شناسایی شما استفاده می شود. اگر کامپیوتر خود را محافظت نکنید این آدرس IP می تواند برای دست یابی به کامپیوتر شما از دنیای اینترنت استفاده شود.

ویروس ها چگونه منتشر می شوند

اگر کسی چیزی در مورد کامپیوتر ها نداند این را می داند که ویروسها مخرب هستند و باید کامپیوتر خود را در برابر هجوم آنها حافظت کند. کمپانی های ضد ویروس (آنتی ویروس) تعداد زیادی ویروس را ساپورت می کنند. ولی هیچ کدام از آنها کامل نیستند. آنتی ویروسهای امروزی بیشتر عمل حفاظت را به طور واکنشی انجام می دهند تا به صورت کنشی. یعنی برای اینکه آنتی ویروس شما متوجه ویروس جدید در کامپیوتر شود باید تا آخرین بیت وارد کامپیوتر شما شود و شروع به فعالیت کند. سناریوی پخش یک ویروس جدید در اینترنت و عکس العمل شرکت های آنتی ویروس در برابر آن به صورت زیر است:

- ابتدا یک ویروس به طور متوسط صد هزار کامپیوتر را مورد هجوم قرار می دهد.
- سپس شرکت های آنتی ویروس شروع به ساختن پکیج برای آنها می کنند.
- در مرحله بعد این پکیج در اختیار عموم قرار می گیرد.

مشکل این است که ممکن است کامپیوتر شما قبل از ساختن این پکیج مورد حمله قرار گیرد. مشکل دیگر این است که اکثر افراد آنتی ویروس کامپیوتر خود را « به روز » یا « up to date » نمی کنند. کمپانی های ضد ویروس بیشتر به صورت اکتشافی عمل می کنند. و این کار را بوسیله برنامه های آشکار سازی انجام می دهند. این برنامه ها کلیه اعمالی را که در کامپیوتر بوسیله برنامه های دیگر انجام می شود تحت نظر می گیرند و هر گاه این اعمال با کارهایی که یک ویروس در کامپیوتر انجام می دهد مطابقت کند آن را به عنوان یک ویروس شناسایی می کنند.سپس جلوی فعالیت آن را می گیرند و همچنین وجود ویروس را به کاربر گوشزد می کنند. با عمل کردن این برنامه آشکار ساز در نرم افزار آنتی ویروس هر گاه یک برنامه فعالیت مشکوکی انجام دهد به کاربر هشدار می دهد و احتمالاً جلوی انتشار ویروس گرفته می شود. این عمل باعث می شود کامپیوتر ها کمتر آلوده شوند.

نرم افزار آنتی ویروس باید به گونه ای تنظیم شود که که روزانه به طور اتوماتیک اجرا شود که شامل به روز کردن و اسکن کردن است .

برنامه های اکتشافی (Heuristics) این فرصت را می دهند که زودتر جلوی انتشار ویروس ها گرفته شود. هر چند استفاده از این برنامه ها یک راه صددرصد فراگیر نیست. ولی بسیار مشکل گشا است. و حساسیت این برنامه ها به

تنظیم سطح حفاظت (Level Setting) در نرم افزار آنتی ویروس بستگی دارد. یعنی آنتی ویروسی که در کامپیوتر شما نصب شده است و تنظیمات آن به شما درکشف ویروسها کمک می کند

ویروسها و مشکلات آنها در اینترنت

ویروسهای کامپیوتری شهرت زیادی در تلوزیون و روزنامه پیدا کرده اند بخصوص اکنون که افراد زیادی از اینترنت استفاده می کنند حتی تصور اینکه کل کامپیوتر شما در اثر بازدید از یک صفحه وب و یا باز کردن یک email بهم ریخته و کارهایتان از بین ربته غیر قابل بخشش است.

یک ویروس تکه code ای است (نوشته می شود بوسیله یک انسان مریض که وقت زیادی دارد) که خود را می چسباند به برنامه های کامپیوتری و خود را منتشر می کند. ویروسها معمولاً اعمال ناخوشایندی روی کامپیوتر و برنامه های آن انجام می دهند. مشکلی که ویروس بوجود می آورد می تواند یک مشکل ساده باشد (مانند باز کردن یک پنجره با یک پیام عاشقانه که هر روز در سر وقت مقرر انجام می شود) یا فوق العاده خطرناک باشد (همه فایلهای موجود در کامپیوترتان را پاک کند) معمولاً زمانیکه کامپیوتر شما به یک ویروس آلوده می شود شما متوجه نمی شوید (اگر آلوده شدن به ویروس آشکار بود نمی توانست به سادگی گسترش پیده کند) احتمالاً کامپیوتر شما شروع به انجام کارهای عجیب و غریب خواهد کرد برنامه ها اجرا نمی شوند فایلهایتان در حال از دست رفتن هستند یا صدمه به کامپیوتر شما وارد می شود.

شما با اجرا کردن برنامه های غیر قابل اعتماد در کامپیوترتان با ویروسها مواجه می شوید ویروسها نمی توانند فایلهی صرفاً اطلاعاتی را آلوده کنند (مثلاً عکسها و فایلهای متن) آنها باید یک برنامه را اجرا کنند تا بتوانند گسترش پیدا کنند.

متاسفانه مرز بین یک فایل اطلاعاتی و یک فایل قابل اجرا خیلی کم رنگ شده است. برای مثال فایلهی Word و Excel می توانند شامل زیر برنامه هایی (Macros) باشند که کارهای مختلفی را انجام می دهند. بنابراین این فایلها می توانند شامل ویروس باشند اگر می خواهید در برابر ویروسها ایمن باشید باید در کامپیوترتان یک آنتی ویروس نصب کنید مطمئن شوید که مرتباً ویروسها را برای آنتی ویروس خود update می کنید (که شامل مشخصات ویروسهای جدید است). باید مواظب فایلهایی که افراد مختلف بوسیله فلاپی دیسکها به شما می دهند باشید یا فایلهایی

که بوسیله e-mail برای شما می فرستند. همیشه نرم افزار شناسایی ویروس را برای هر فایلی که از آن مطمئن نیستید اجرا کنید به یاد داشته باشید که دیگران همیشه می توانند فایلهای ویروسی را به شما انتقال دهند بدون اینکه درباره آنها اطلاعی داشته باشند بنابراین فقط به دلیل اینکه این فایل از مطمئن ترین دوست شما گرفته شده است به این معنی نیست که حتماً ویروسی نیست!

آنتی ویروس کامپیوتر شما را از ویروسها در امان نگه می دارد

فرهنگ جامع ویروس جدیدترین اطلاعات را از آخرین ویروسها در خود دارد

بعید است که شما با بازدید از یک وب سایت با ویروس مواجه شوید. بعضی از صفحات وب شامل کدهای برنامه نویسی هستند (مثلاً جاوا اپلتها یا جاوا اسکریپتها) اما معمولاً مشکلی پیش نمی آید اگر چه حفره های قابل نفوذ مخربی در مرورگرهای وب پیدا شده است و این مرورگرها ممکن است نمونه ای از ویروسهایی که که ممکن است بر اساس یک جاوا اسکریپت نوشته شود را در خود نداشته باشند.بنابراین برای در امان بودن مطمئن شوید که هر تکه (patch) در دسترس را برای مرورگر (browser) خود download کرده اید.

شوخی های مزاحم درemail

یک مشکل بسیار گسترده در اینترنت وجود دارد و آن پیغامهای الکترونیکی که در مورد یک ویروس هشدار می دهند و این هشدار در مورد یک email با یک عنوان (subject) مشخص می باشد که این email ها ویروس های خطرناک هستند و به کامپیوتر شما آسیب می رسانند.

مثال:

Please do not open up any mail that has this title.
It will erase your whole hard drive. This is a new
e-mail virus and not a lot of people know about
it, just let everyone know, so they won't be a victim.
Please forward this e-mail to you friends!!!
Remember the title: JOIN THE CREW.

مثال دیگر:

Subject: VIRUS WARNING VERY IMPORTANT
Please read the following message we received from a client.
If you receive an email titled "It Takes Guts to Say 'Jesus'"
DO NOT open it. It will erase everything on your hard drive. So, you must delete it.
Forward this E-MAIL out to as many people as you can. This is a new, very

malicious virus and not many people know about it. This information was announced yesterday morning from IBM; please share it with everyone that might access the internet. Once again, pass this along to EVERYONE in your address book so that this may be stopped. AOL has said that this is a very dangerous virus and that there is NO remedy for it at this time.
Please practice cautionary measures.

اگر شما email ای مانند این دیدید آن را برای کسی نفرستید! ویروسهای "Jion The Crew" و " It Takes to Say 'Jesus Guts'" شوخی هستند! ویروسهای شوخی دیگری وجود دارند مانند:

"Win a Hliday" , "AOL4Free" , "Pen Pal Greetings", "ghost" , "Deeyenda"

و بد نام ترین آنها "Good times" است.

ویژگیهای اخطار ویروسهای شوخی:

- تأکید بسیار
- یک هشدار که ویروس فقط با باز کردن پیغام فعال می شود (شما نمی توانید فقط با باز کردن یک پیفام آلوده شوید مگر اینکه یک پیوست (attachment) را باز کنید.
- کلمات « این یک ویروس جدید است که بسیاری از مردم آن را نمی شناسند » در آن دیده می شود
- دستور العملها به شما می گویند که با دنبال کردن یک لینک آن را برایکسانیکه می شناسید بفرستید.
- با اشاره به اینکه ویروس روز قبل بوسیله یک شرکت یا گروه کامپیوتری معتبر مانند "IBM" یا "Microsoft" و یا ... اعلام شده است می خواهند هشدار خود موجه جلوه دهند.

در اینجا یک مثال از یک هشدار حقیقی در مورد ویروس وجود دارد:

Hi all,
There is a virus (a "worm", actually) currently doing the rounds that comes packaged in a file called PrettyPark.exe attached to an email.

Apparently it has been around since May last year, but has proliferated recently and is currently by far the most "popular" subject of enquiries at Symantec's anti-virus research center.
The usual rules apply: don't open it.
Information (including a fix if you are infected) is available at this site:
http://www.symantec.com/avcenter/venc/data/prettypark.worm.html
Good luck, Take care.

ویژگیهایی که نشان می دهند این ویروس مربوط به یک ویروس واقعی است عبارتند از :

- پیغام به شکل ساده و زبان منطقی و مستدل بیان شده است (بدون هیچگونه بزرگنمایی در لغات)
- پیغام در مورد باز کردن یک بایل الصاقی (attachment) هشدار نی دهد
- پیغام آدرس سایت معتبری را می دهد که در آن می توانید در مورد ویروس اطلاعات بیشتری پیدا کنید.
- در پیغام اطلاعاتی در مورد اینکه اگر کامپیوتر شما آلوده به ویروس شد چه کار باید انجام دهید به شما اطلاعاتی میدهد.
- در پیغام از شما خواسته نمی شود که آن را برای کسی بفرستید.

کرمها(worms)

کرمها اصولاً ویروس نیستند با این وجود تفاوت بین آنها بسیار اندک است و معمولاً در اخبار روزمره آنها را با یکدیگر اشتباه می گیرند. ویروسها یک کامپیوتر منفرد را آلوده می کنند وسعی نمی کنند به کامپیوتر دیگری راه پیدا کنند کرمها به کامپیوترهای دیگر انتقال پیدا می کنند با اعمال شما. (مثلاً با اشتراک گذاشتن فایلها بوسیله email یا بوسیله فلاپی دیسک ها کرمها به شدت علاقه مندند که فقط خود را در میان یک شبکه گسترش دهند. آنها به طور خود کار خودشان را به کامپیوترهای دیگر انتقال می دهند به علت اینکه انتقال آنها بین کامپیوترها به طور خودکار انجام می پذیرد سرعت گسترش آنها بسیار سریعتر از ویروسها است.

معمولترین راه گسترش یک کرم این است که خود را به همه آدرسهای email ای که شما در address book خ.د لیست کرده اید برساند یا outlook شرکت مایکروسافت برنامه email ای است که بیشترین آسیب پذیری را در برابر حمله کرمها دارد فقط به این دلیل که عمومی ترین برنامه است برای کاهش دادن احتمال آلوده شدن به کرمها شما می توانید مراحل زیر را اجرا کنید:

- هیچ فایل الصاقی (attachment) غیر منتظره ای را در email های خود باز نکنید (بخصوص آنهایی را که شامل پیغامهای معمول مانند در این جا فایلی که شما درخواست کرده اید وجود دارد.) هر چند آنها از منابع مطمئنی برای شما ارسال شده باشند. برای فرستنده email ای بفرستید (reply) و از او سئوال کنید او واقعاً چنین فایلی برای شما فرستاده است یا نه؟
- یک آنتی ویروس نصب کنید و آن را مرتباً up to date کنید.
- اگر ممکن است از نرم افزار email ای به قیر از Express Outlook استفاده کنید.

کرمی که به خوبی منتشر شده "Love Letter" نام دارد که با فرستادن خود به آدرس email ای که در address book نرم افزار Outlook Express وجود دارند منتشر می شود به راحتی کپی کردن فایل در

کامپیوتر قربانی خود را وارد می کند و با یک عنوان به صورت "I LOVE YOU" وارد می شود و پیغام آن به صورت زیر است :

"Rindly chek the attached LOVE LETTER coming from me"

بدلیل اینکه email از یک فرد شناخته شده برای گیرنده ارسال شده است بسیاری از مردم گول می خورند و کرم در حجم وسیع گسترش پیدا می کند. اگر چه به کامپیوتر قربانی آسیب وارد می شود ولی آسیب اصلی به کل شبکه وارد می شود و همه آن را آلوده می کند.

اسب تراوا چیز جالبی بنظر می رسد اما چیزهای آسیب رسان و کثیفی در بر دارد. و در لباس خدمات مفید یا پیوستهای (attachments) جذاب در email مثلاً یک screen saver پخش می شود. آنها فایلهی الصاقی برای شما می فرستند که آنقدر برای شما جالب است که آنها را برای دوستانتان می فرستید. در حالیکه آثار مخرب آن پنهان بوده با تأخیر عمل می کند بنابراین شما نمی دانید چیزی که در حال فرستادن آن هستید یک فایل خطرناک است.

در مواقع دیگر این کرمها تکثیر می شوند مانند یک کرم اینترنتی و خود را به صورت اتوماتیک به کامپیوترهای دیگر می رسانند و معمولاً از Outlook Express استفاده می کنند.

امنیت در اینترنت:

امنیت در اینترنت مهم است بخصوص برای کودکان اگر شما صاحب فرزندانی هستید که نگران گشت گذار آنها در اینترنت هستید که ممکن است از سایتهای غیر اخلاقی سر در بیاورند. ممکن است بخواهید از نرم افزارهای فیلترینگ استفاده کنید. نرم افزارهای فیلترینگ می توانند بیشتر سایتهای ناشایست را مسدود کنند و معولاً می توان آنها را بوسیله یک password غیر فعال کرد. یک مشکل نرم افزارهای فیلترینگ این است که تعدادی از سایتهای بدون مشکل را هم مسدود می کنند مثلاً زمانیکه اطلاعاتی در مورد سرطان سینه بخواهید ممکن است این نرم افزار لغت سینه را به عنوان یک لغت ناشایست منظور کند. موارد دیگر برای امنیت در اینترنت به قرار زیر است:

- در سایتهای شخصی یا در هنگام chat اطلاعاتی مانند آدرس خود یا شماره تلفن خود را در اختیار دیگران قرار ندهید.
- اگر شما chat می کنید یا با شخصی بوسیله e-mail که به او اطمینان کامل ندارید ناحیه ای را که منطقه مورد سکونت خود را به او اطلاع ندهید.

- اطلاعات شخصی از قبیل آدرس یا شماره حساب بانکی یا شماره کارت اعتباری را در email ها وارد نکنید یا آنها را در فیلدهای خواسته شده در یک سایت غیر ایمن وارد نکنید بنابراین همیشه قبل از دادن این

اطلاعات مطمئن شوید در یک سایت ایمن هستید و بعد شماره کارت اعتباری خود را برای خرید وارد کنید. تشخیص یک سایت ایمن از غیر ایمن معمولاً بسیار ساده است زیرا یک سرور ایمن با "https://" در فیلد آدرس ظاهر می شود و حال آنکه یک سرور غیر ایمن با "http://" شروع می شود سرورهای ایمن اطلاعات شما را به رمز در می آورند.بنابراین هیچکس به غیر از شما و کامپیوتری که در سمت دیگر است نمی تواند این اطلاعات را در یافت کند.

- از یک ویروس یاب استفاده کنید. از سایتهای غیر مطمئن یا email های مشکوک فایلی Doanload نکنید. حتی اگر یک ویروس یاب دارید خیلی مواظب باشید زیرا ممکن است با ویروس جدیدی مواجه شوید که نرم افزار ضد ویروس شما نتواند آن را تشخیص دهد برای یک یک حفاظت خوب همیشه آنتی ویروس خود را) up date به روز (نگه دارید.

فایروال (firewall) چیست؟

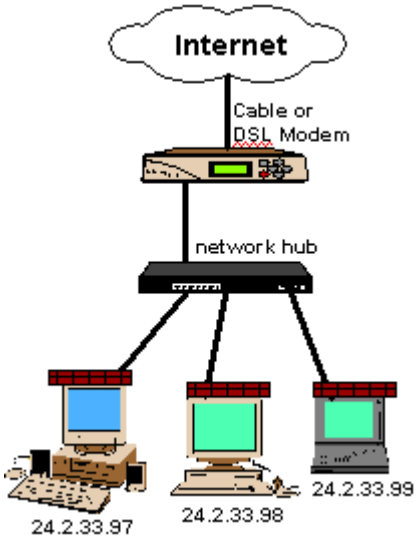
یک فایروال از شبکه شما در برابر ترافیک ناخواسته و همچنین نفوذ دیگران به کامپیوتر شما حفاظت می کند .توابع اولیه یک فایروال به این صورت هستند که اجازه می دهند ترافیک خوب عبور کند و ترافیک بد را مسدود می کنند! مهمترین قسمت یک فایروال ویژگی کنترل دستیابی آن است که بین ترافیک خوب و بد تمایز قائل می شود .

وقتی آن را نصب می کنید فایروال بین کامپیوتر شما و اینترنت قرار می گیرد. فایروال به شما اجازه می دهد صفحات وب را ببینید و به آنها دسترسی داشته باشید، فایل download کنید، چت کنید و . ... در حالیکه مطمئن هستید افراد دیگری که در اینترنت مشغول هستند نمی توانند به کامپیوتر شما دست درازی کنند. بعضی از فایروالها نرم افزارهایی هستند که روی کامپیوتر اجرا می شوند اما فایروالهای دیگر به صورت سخت افزاری ساخته شده اند و کل شبکه را از حمله مصون می کنند.

هر کسی که از اینترنت استفاده می کند باید از بعضی از انواع فایروالها استفاده کند. برنامه هایی هستند که می توانند از اینترنت download شوند این برنامه ها می توانند تعداد زیادی آدرسهای IP آسیب پذیر برای نفوذ را پیدا می کنند این برنامه ها به راحتی download شده و اجرا می شوند و برای سوء استفاده یا مشکل دار کردن کامپیوتر شما از طریق این برنامه ها احتیاجی به دانش شبکه نیست معمولاً همه انواع فایروالها از شما در برابر این حملات حفاظت می کنند.

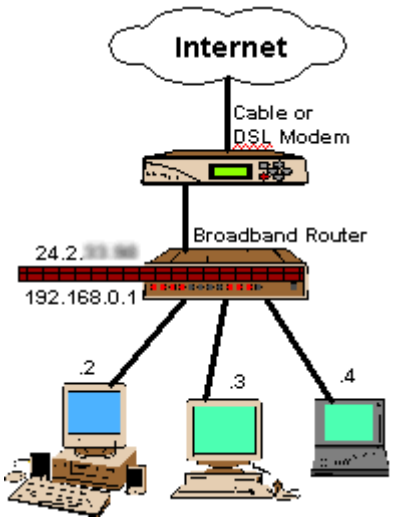
فایروالهای نرم افزاری

فایروالهای نرم افزاری برنامه هایی هستند که خود را بین درایو کارت شبکه (یا مودم) و کامپیوتر شما قرار می دهند. آنها حملات را قبل از اینکه حتی سیستم شما آن را تأیید کند قطع می کنند. تعداد زیادی فایروالهای مجانی از این نوع روی اینترنت وجود دارند.



فایروال NAT ساده

فایروالهایی که برای broadband router ها ساخته شده اند و نرم افزارهایی مانند Microsoft ICS فایروالهای بسیار ساده ای هستند. و این فایروالها شبکه را با جلوگیری از ارتباط مستقیم هر کامپیوتر با کامپیوترهای دیگر شبکه محافظت می کنند. این نوع فایروالها تقریباً هر نوع هکری را متوقف می کنند. هکرهای حرفه ای ممکن است بتوانند از این فایروالها عبور کنندااما تعداد چنین اشخاصی کم و احتمال آن ضعیف است.



فایروالهای با ویژگی stateful packet inspection

نسل جدید فایروالهای خانگی stateful packet inspection نامیده می شوند. این یک شکل پیشرفته از فایروال است که هر پاکت اطلاعاتی را که از فایروال عبور می کند بازرسی می کند. فایروال هر پاکت اطلاعاتی را برای ردیابی هر نوعی از هک اسکن می کند.بیشتر افراد هرگز با این نوع حمله ها روبرو نمی شوند اما نواحی در اینترنت وجود دارند که بیشتر مورد حمله هکرهای حرفه ای واقع می شوند