ویـــژه
امنـــیت

امنیـــت کامپیـــوتر از ســـیر تا پـــیاز

یکی از اشـــکالاتی که همیشه کشـــورهای جهان سوم را رنج می‌دهد آن اســـت که همواره اقدام به ورود فناوری جدید از کشـــورهای توســـعه‌یافته می‌کنند، بدون آنکه فرهنگ اســـتفاده از آن را هم وارد کنند! هر کســـی با نگاهی گذرا به پیرامون خود درستی این مسئله را تایید می‌کند. از نحوه استفاده از وسیله نقلیه شخصی گرفته تا نحوه استفاده از اینترنت، همگی گواه این مدعا هستند.

برای آنکه خیلی وارد مسایل اجتماعی نشویم و در حوزه تخصصی این ماهنامه حرکت کنیم، به امنیت کامپیوتر اشـــاره می‌کنیم. امنیت کامپیوتر موضوعی اســـت که ویژه‌نامه این شـــماره ماهنامه را به خود اختصاص داده و مصداق صحبت بالا است.

اغلـــب کاربران کامپیوتر، یـــا به امنیت کامپیوتر خود توجهی ندارند و یا خیلی به اهمیت آن واقف نیســـتند. امنیت کامپیوتر برای بســـیاری از کاربران مصداق واقعی نوش‌دارو پس از مرگ ســـهراب اســـت! یعنی آن زمانی که به دلیل ضعف امنیتی دچار انواع و اقســـام مشـــکلات شده‌اند، تازه به دنبال راه چاره می‌گردند که البته در اغلب موارد کار چندانی نمی‌توان کرد.

برخـــلاف تصور بســـیاری از کاربران، امنیـــت کامپیوتر فقط در ضدویروس خلاصه نمی‌شـــود، بلکه عناوین مهم دیگری مثل نرم‌افزارهای ضدجاسوســـی، فایروال‌ها، نرم‌افزارهای کنترل پســـوردها، نرم‌افزارهای رمزنگاری اطلاعات، نرم‌افزارهای امنیت در اینترنت، نرم‌افزارهای کنترل والدین بر فرزنـــدان، نرم‌افزارهای مانیتورینگ و ... مجموعا امنیـــت کامپیوتر را تضمین می‌کنند، البته نه ۱۰۰ درصد!

مـــا در ایـــن ویژه‌نامه قصد داریـــم در حدی که با محدودیـــت صفحه مواجه نشـــویم، به رئوس موارد امنیتی اشـــاره کنیم و در این راه موارد لازم را گروه‌بنـــدی کرده و عملکرد هر گـــروه را توضیح داده و سپس در قسمت‌های آتی با یکی از نرم‌افزارهای مطرح در آن گروه آشنا شویم.

آنتی‌ویروس، لازم اما ناکافی!

هومن سیاری
Sayyari@ComputerNews.ir

بسیاری از کاربران تصور می‌کنند با نصب یک ضدویروس یا همان آنتی‌ویروس، زره ضدگلوله بر تن کامپیوترشان کرده‌اند و دیگر هیچ تهدیدی وجود ندارد. این تصور غلط بلای جان بسیاری از کاربران می‌شود. دلایل زیادی برای اثبات این مدعا وجود دارد:

● هیچ کدام از ضدویروس‌ها توانایی مقابله و حذف تمامی ویروس‌ها را ندارند. هرچند اغلب ضدویروس‌های حرفه‌ای امکان مقابله با درصد بالایی از ویروس‌ها را دارند، اما این توان هیچ‌گاه ۱۰۰ درصد نیست. برای آگاهی از کیفیت و توانایی ضدویروس مورد نظرتان به سایت‌های تخصصی بررسی و مقایسه ضدویروس‌ها از جمله www.av-comparatives.org مراجعه کنید.

● همواره ویروس‌ها از ضدویروس‌ها جلوترند. بدیهی است همیشه ابتدا ویروس ساخته می‌شود و پس از مدتی شرکت‌های امنیتی اقدام به ساخت ضدویروس آن می‌کنند. بنابراین بهترین ضدویروس هم در مقابل ویروس‌های جدید خلع سلاح است!

● آپدیت ضدویروس هم از آن دست مسایلی است که کاربران ایرانی توجه کمتری به آن دارند. اگر یک ضدویروس آپدیت نشود، به معنای این است که نمی‌تواند ویروس‌هایی جدیدی را که از زمان آخرین آپدیت ضدویروس ساخته شده‌اند و ضدویروس آنها هم عرضه شده، شناسایی کرده و در مقابل آنها بایستد. از مهم‌ترین دلایلی که کاربران ایرانی از آپدیت ضدویروس خود غفلت می‌کنند، می‌توان به سرعت پایین اینترنت و استفاده از ضدویروس‌های کرک‌شده اشاره کرد.

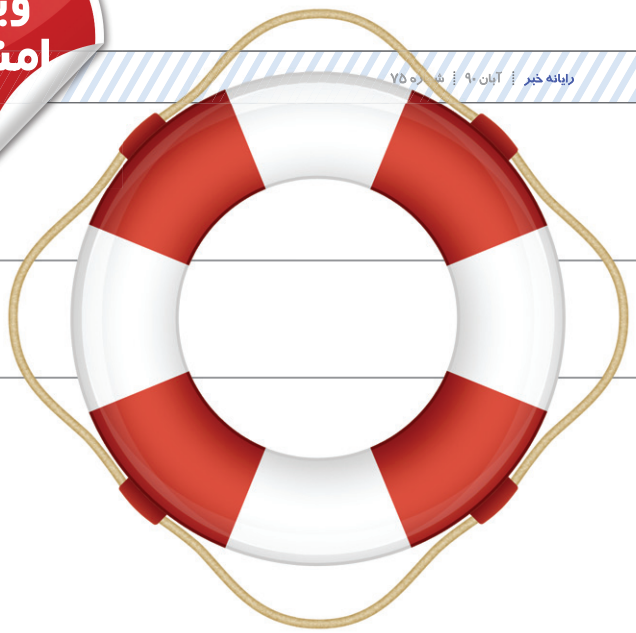
● ضدویروس کرک‌شده (قفل‌شکسته) هم مورد مهم دیگری است که خیل عظیمی از کاربران به آن توجه نمی‌کنند. اصولا ما کاربران ایرانی علاقه‌ای به خرید نرم‌افزار اوریجینال نداریم و عادت کرده‌ایم هر نرم‌افزاری را به صورت کرک‌شده و البته رایگان مورد استفاده قرار دهیم. هر چند ترک این عادت کاری بسیار مشکل است، اما توصیه می‌شود حداقل ضدویروس را به صورت اوریجینال تهیه کنید. بسیاری از ضدویروس‌های تقلبی در ظاهر آپدیت می‌شوند، اما عملکرد صحیحی ندارند.

● هر شرکتی ضدویروس خود را در نسخه‌های متفاوت عرضه می‌کند. نسخه‌های ساده فقط ضدویروس هستند، اما نسخه‌های کامل‌تر مثل نسخه‌های Internet Security و Total Security علاوه بر ویروس‌ها می‌توانند در مقابل کرم‌ها و جاسوس‌ها و ... هم مقابله کنند. طبیعتا این نسخه‌ها گران‌تر بوده، اما در عوض امن‌ترند.

● بعضی از کاربران از ضدویروس اوریجینال استفاده می‌کنند، از نسخه رایگان آن! هر چند استفاده از نسخه رایگان خیال شما را از بابت آپدیت راحت می‌کند، اما مشکل این است که هیچ شرکتی در راه رضای خدا محصول گران‌قیمتش را به صورت رایگان عرضه نمی‌کند. ضدویروس‌های رایگان معمولا از حداقل امکانات برخوردارند و حتی برخی از آنها توانایی یافتن ویروس‌ها را به صورت خودکار ندارند.

● حتی در صورت استفاده از یک ضدویروس اوریجینال که مدام آپدیت می‌شود، باز در معرض خطر هستید، چرا که بسیاری از مشکلات امنیتی از طریق حفره‌های امنیتی سیستم‌عامل و به خصوص ویندوز ایجاد می‌شود. بنابراین باید پیوسته اقدام به آپدیت سیستم عامل کنید که این هم مستلزم داشتن ویندوز اوریجینال است. مشکلی که به این راحتی‌ها برای ما کاربران ایرانی قابل هضم نیست، چرا که پرداخت بیش از ۱۰۰ هزار تومان برای ساده‌ترین نسخه ویندوز۷ با فرهنگ کامپیوتری ما ناسازگار است!

● استفاده از شبکه‌های اجتماعی مثل فیس‌بوک و توییتر بستر مناسبی را برای سرقت اطلاعات فراهم می‌کند که ضدویروس نمی‌تواند نقش موثری در این زمینه بازی کند. ■



دیسک نجات

آخرین منجی سیستم شما از شر ویروس‌ها

فکر نمی‌کنیم کاربری یافت شود که با ویروس‌های کامپیوتری مواجه نشده باشد. تقریبا تمامی کاربران، حتی حرفه‌ای‌ترین آنها چند باری با انواع و اقسام ویروس‌ها دست و پنجه نرم کرده‌اند و شاید خیلی از آنها مشکلات و خسارات فراوانی در این زمینه دیده باشند؛ از پاک شدن فایل‌های مهم تا اجبار به نصب مجدد ویندوز و ... همگی می‌دانیم که تنها راه مقابله با ویروس، نصب ضدویروس روی کامپیوتر است. اما مشکل این است که حتی در این صورت هم ممکن است سیستم شما دچار ویروس شود. شاید بپرسید پس راه حل نهایی چیست؟

در این باره می‌توان یک مقاله جداگانه نوشت اما به اختصار می‌توان به پارامترهای زیر اشاره کرد:

نصب یک ضدویروس قوی اوریجینال، آپدیت دایمی ضدویروس، اسکن حافظه‌های فلش و سی‌دی‌ها و دی‌وی‌دی‌ها قبل از استفاده، عدم مراجعه به سایت‌های مشکوک، باز نکردن ایمیل‌های ناشناس، استفاده از فایروال و ...

حتی اگر تمامی موارد بالا را به کار بسته باشید، باز هم احتمال ویروسی شدن سیستم وجود دارد. یک نکته مهم را همیشه به یاد داشته باشید: ویروس‌ها همیشه از ضدویروس‌ها جلوترند! همیشه ابتدا ویروس ساخته می‌شود و کلی خرابکاری در سراسر دنیا می‌کند و سپس شرکت‌های سازنده ضدویروس اقدام به ساخت ضدویروس آن می‌کنند!

دیسک نجات چیست؟

گاهی اوقات ویروس روی فایل‌های سیستمی ویندوز می‌نشیند و آنها را آلوده می‌کند. در این شرایط حتی اگر ضدویروس بتواند آن ویروس را تشخیص دهد، باز هم قادر به پاک کردنش نیست، چرا که ویندوز اجازه دسترسی به فایل‌های سیستمی خود را به هیچ نرم‌افزاری حتی ابزارهای ضدویروس نمی‌دهد. این چیزی است که شاید خیلی از شما کاربران کامپیوتر با آن مواجه شده باشید، ویروس‌هایی که پیدا می‌شوند اما پاک نمی‌شوند!

در این شرایط نهایت هنری که ممکن است ضدویروس از خود به خرج دهد، قرنطینه کردن آن فایل آلوده است. قرنطینه کردن مثل زندانی کردن فایل است، یعنی اجازه فعالیت به فایل داده نمی‌شود.

چه فایل آلوده قرنطینه بشود و چه نشود، در هر دو حالت مشکلاتی به وجود می‌آید. اگر قرنطینه بشود، جلوگیری از فعالیت عادی آن فایل منجر به عدم کارکرد ویندوز خواهد شد و مدام با انواع و اقسام پیام‌های خطا مواجه می‌شوید و اگر قرنطینه نشود، آن ویروس با آرامش خاطر اقدام به فعالیت مخرب خود خواهد کرد!

در چنین شرایطی است که دیسک‌های نجات (Rescue Disk) به کمک شما می‌آیند. دیسک‌های نجات در واقع سی‌دی یا دی‌وی‌دی یا حافظه فلش قابل بوت هستند که از طریق آنها کامپیوتر را بوت کرده و سپس اقدام به ویروس‌یابی می‌کنید. در این حالت چون ویندوز فعال نیست، نمی‌تواند مانع فعالیت ضدویروس و دسترسی آن به فایل‌های سیستمی شود و ضدویروس با خیالی آسوده تمامی فایل‌های آلوده را تمیز خواهد کرد!

توجه: این احتمال وجود دارد که دیسک نجات، بعضی از فایل‌های مهم سیستم‌عامل ویندوز را پاک کند. دلیل آن این است که نتوانسته ویروس را از روی فایل پاک کند و مجبور شده کل فایل را پاک نماید. در چنین شرایطی امکان دارد ویندوز دیگر بالا نیاید!

پس قبل از استفاده از دیسک نجات، حتما از فایل‌های مهم خود پشتیبان تهیه نمایید.

دیسک نجات ضدویروس کسپرسکی

تقریبا تمامی ضدویروس‌های معتبر دیسک نجات هم دارند. چون ضدویروس کسپرسکی جزو بهترین ضدویروس‌های دنیاست و کاربران بسیاری از آن استفاده می‌کنند، بر آن شدیم تا طریقه ساخت دیسک نجات این ضدویروس را در این مقاله تشریح کنیم. لازم به ذکر است که دیسک نجات قابلیت ویروس‌یابی سیستم‌های ۳۲ بیتی و ۶۴ بیتی را به طور همزمان داراست.

مواد لازم!

۱. یک درایو سی‌دی یا دی‌وی‌دی برای اجرای دیسک نجات
۲. یک سی‌دی‌رایتر یا دی‌وی‌دی‌رایتر برای ساخت دیسک نجات (یا یک پورت USB برای اجرا و ساخت حافظه فلش نجات)

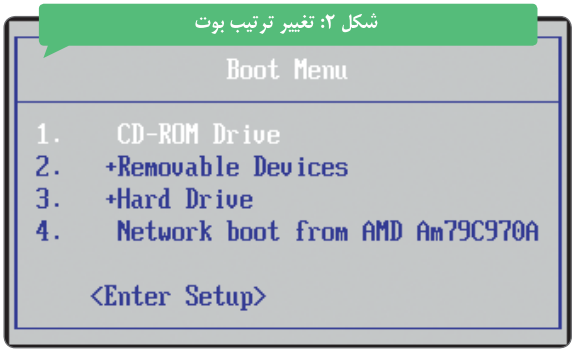
۳. مادربورد امکان بوت از طریق سی‌دی یا USB را داشته باشد
۴. ویندوز ایکس‌پی با سرویس‌پک۲ به بالا یا ویندوز ویستا یا ویندوز۷

طریقه ساخت دیسک نجات کسپرسکی

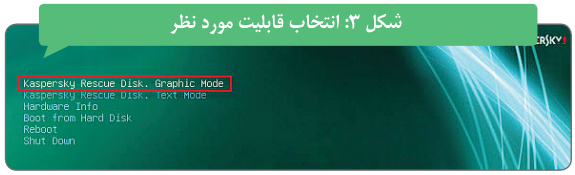
۱. ابتدا باید فایل ایمیج دیسک نجات کسپرسکی را از سایت کسپرسکی دانلود کنید (حجم این فایل حدود ۲۰۵ مگابایت است که برای سهولت آن را در دی‌وی‌دی همین شماره ماهنامه رایانه‌خبر قرار داده‌ایم).

شکل ۱: رایت ایمیج توسط Nero

شکل ۲: تغییر ترتیب بوت



شکل ۳: انتخاب قابلیت مورد نظر



۲. این ایمیج را روی یک سی‌دی یا دی‌وی‌دی رایت نمایید (اگر روی سیستم ضدویروس کسپرسکی ۲۰۱۲ را دارید، در خود این نرم‌افزار بخشی تعبیه شده که این فایل ایمیج را روی سی‌دی یا دی‌وی‌دی رایت می‌کند. اگر این نسخه از ضدویروس را ندارید، با هر نرم‌افزار دلخواهی مثل Nero می‌توانید کار رایت را انجام دهید – شکل ۱).
- سعی کنید دیسک نجات را با سرعت پایین رایت کنید.
- دقت نمایید فایل مذکور یک فایل ISO است و باید در نرم‌افزار رایت آن را به صورت ایمیج رایت نمایید.

۳. تغییر ترتیب بوت در Setup کامپیوتر
برای وارد شدن در Setup مادربورد باید یکی از دکمه‌های Del، F10، F2 یا ... را هنگام بوت بفشارید. برای مشخص کردن دکمه مورد نظر به دفترچه راهنمای مادربورد مراجعه کنید.
بعد از ورود به Setup به دنبال جایی بگردید که ترتیب بوت را مشخص می‌کند و سپس سی‌دی یا دی‌وی‌دی را به گزینه اول منتقل کنید و تغییرات را ذخیره کنید (شکل ۲).

۴. سی‌دی یا دی‌وی‌دی نجات را در درایو قرار داده و کامپیوتر را مجدد راه‌اندازی کنید. یک دکمه دلخواه را بفشارید. اگر انتخاب شما بیش از ۱۰ ثانیه طول بکشد، کامپیوتر به طور خودکار از روی هارددیسک بوت خواهد شد و وارد ویندوز خواهید شد (شکل ۳).

۵. صفحه دیگری به نمایش در خواهد آمد که باید در آن زبان مورد نظر را انتخاب نمایید.
۶. در صفحه بعدی باید یکی از موارد نمایش‌داده‌شده را انتخاب کنید:
- ورود به برنامه دیسک نجات در قالب محیط گرافیکی
- ورود به برنامه دیسک نجات در قالب محیط متنی
- نمایش مشخصات سخت‌افزاری سیستم
- بوت از روی هارددیسک
- بوت مجدد سیستم
- خاموش کردن کامپیوتر

طریقه ساخت حافظه فلش نجات کسپرسکی

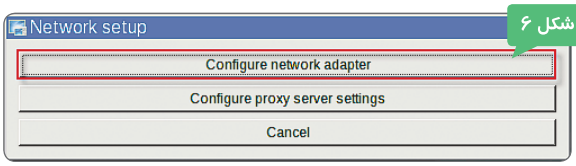
۱. حافظه فلش را به یک پورت USB متصل کنید (این فلش حداقل باید ۲۵۶ مگابایت ظرفیت داشته باشد و فایل‌سیستم آن FAT16 یا FAT32 باشد. اگر فایل‌سیستم آن NTFS بود از طریق فرمت ویندوز آن را به FAT32 تبدیل کنید).
۲. اکنون نرم‌افزار دیگری تحت عنوان rescue2usb.exe را اجرا نمایید. این نرم‌افزار برای ساخت حافظه فلش نجات لازم است و ما آن را نیز در دی‌وی‌دی همین شماره ماهنامه رایانه‌خبر قرار داده‌ایم.
۳. از طریق دکمه Browse آدرس فایل ایمیج مخصوص ساخت حافظه فلش نجات را به این ابزار بدهید (این فایل را نیز در دی‌وی‌دی همین شماره می‌توانید بیابید). البته از همان فایل نجاتی که برای ساخت سی‌دی استفاده می‌شود نیز می‌توان برای ساخت حافظه فلش نجات استفاده کرد.
۴. سپس از بخش پایین، حافظه فلش خود را انتخاب نمایید.
۵. اکنون دکمه بزرگ Start را بزنید. عملیات کپی آغاز می‌گردد و در پایان پیام انجام کار نمایش داده می‌شود (شکل ۴).
۶. حال باید مراحل ۳ تا ۶ بخش قبلی را عینا تکرار کنید، با این تفاوت که در مرحله ۳ باید حافظه فلش را به عنوان انتخاب اول برای بوت در نظر بگیرید.

آپدیت دیسک نجات

تنها مشکلی که در این جا وجود دارد این است که فایل ایمیجی که از روی آن دیسک نجات یا حافظه فلش نجات را ساختیم، مربوط به چند ماه قبل است و

شکل ۴: رایت فایل ایمیج دیسک نجات روی حافظه فلش

شکل ۵



شکل ۶

شکل ۷

شرکت کسپرسکی آن را آپدیت نکرده است. بنابراین احتمالا نمی‌تواند ویروس‌های جدیدی که در این چند ماه ساخته شده‌اند را پاک کند. برای این منظور حتما باید ابتدا دیسک نجات یا حافظه فلش نجات خود را آپدیت کنیم وسپس اقدام به استفاده از آن نماییم.

برای آپدیت دیسک نجات ۲ راه دارید: یا کامپیوتر مورد نظر دسترسی به اینترنت دارد و یا فایل‌های آپدیت ضدویروس را قبلا تهیه کرده‌اید.

- **دانلود آپدیت**

۱. کامپیوتر را توسط دیسک نجات یا حافظه فلش نجات بوت کنید و وارد بخش گرافیکی شوید و دکمه استارت آن را فشرده و گزینه Network Setup را انتخاب کنید (شکل ۵).

۲. تنظیمات کارت شبکه را برای اتصال به اینترنت انجام دهید (دقیقا همان تنظیماتی که کارت شبکه در محیط ویندوز دارد را اعمال نمایید). با اعمال صحیح تنظیمات، پیام موفقیت به نمایش در خواهد آمد (شکل ۶).

۳. دوباره دکمه استارت را فشرده و گزینه Kaspersky Rescue Disk را انتخاب کنید و از برگه My Update Center گزینه Start Update را انتخاب کنید.

- **اعمال فایل‌های آپدیت از پیش آماده**

اگر از قبل فایل‌های آپدیت را دانلود کرده‌اید و نمی‌خواهید دوباره فرایند آپدیت را طی کنید، مراحل زیر را انجام دهید:

۱. فایل‌های آپدیت را در فولدری دلخواه در همان کامپیوتر و یا در حافظه فلش نجات کپی کنید.

۲. کامپیوتر را از روی دیسک نجات یا حافظه فلش نجات بوت کنید و وارد بخش گرافیکی شوید و دکمه Settings را در بالای سمت راست برنامه کلیک نمایید (شکل ۷).

۳. گزینه MyUpdate Center را انتخاب کنید و سپس از بخش سمت راست گزینه Settings را برگزینید (شکل ۸).

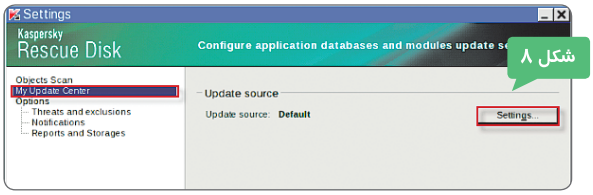
۴. از بخش Source گزینه Add را انتخاب کنید و سپس آدرس فولدر مرحله ۱ را انتخاب کنید و Ok کنید و از پنجره‌ها خارج شوید (شکل ۹).

۵. دوباره دکمه Start را کلیک کرده و گزینه Kaspersky Rescue Disk را انتخاب کنید و از برگه My Update Center گزینه Start Update را انتخاب کنید.

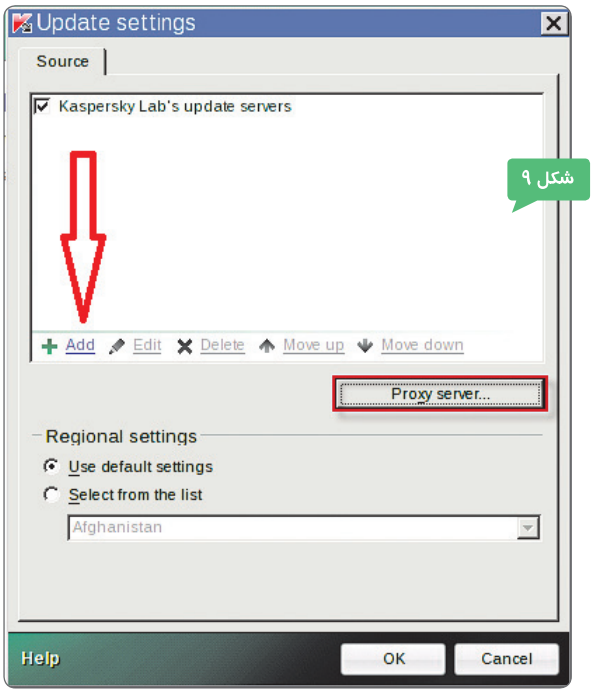
نکته: اگر کامپیوتری دیگری دارید که ضدویروس کسپرسکی دارد و آپدیت هم هست، برای اینکه درگیر آپدیت دیسک نجات نشوید و مجبور نباشید با استفاده از اینترنت کند خود مدتی معطل آپدیت آن شوید، مراحل زیر را انجام دهید:

۱. ضدویروس آن کامپیوتر را باز کنید و در بخش UpdateCenter به دنبال قسمت Copy update to folder بگردید. آدرس مشخص شده در آن بخش را یادداشت کنید.

۲. آن کامپیوتر را با استفاده از دیسک نجات و یا حافظه فلش نجات بوت کنید و مطابق بخش قبل (اعمال فایل‌های آپدیت از پیش آماده) با استفاده از آدرس مرحله ۱ اقدام به آپدیت نمایید. ■



شکل ۸



شکل ۹

Spyware چیست؟

هومن سیاری
Sayyari@ComputerNews.ir

Spyware چیست؟

Spyware یا جاسوس‌افزار برنامه‌هایی هستند که به صورت پنهانی و با اهدافی نظیر جاسوسی، تبلیغات، خرابکاری و ... روی سیستم فعالیت می‌کنند. در ادامه به بررسی بیشتر هر یک از انواع آنها می‌پردازیم:

- جاسوس‌افزار نوعی از برنامه‌های مخرب است که به طور خودکار روی کامپیوتر نصب شده و اطلاعات کاربر آن کامپیوتر را بدون اطلاع وی جمع‌آوری کرده و برای مقصد نامشخصی ارسال می‌کند. این دسته از جاسوس‌افزارها با هدف **جاسوسی** طراحی شده‌اند.

- برخی از گونه‌های آن آگهی‌های تبلیغاتی ناخواسته نمایش می‌دهند که به آنها adware نیز گفته می‌شود. هدف از این دسته از جاسوس‌افزارها، بیشتر **تبلیغات** کالاهای مختلف به خصوص کالاهای غیرمجاز و غیراستاندارد است. این تبلیغات به صورت ناخواسته و به صورت پیاپی ظاهر می‌شوند، حتی زمانی که به اینترنت متصل نیستید.

- گونه دیگری از جاسوس‌افزارها هم اقدام به تغییر خودکار تنظیمات ویندوز می‌کنند. هدف از طراحی این دسته از جاسوس‌افزارها بیشتر **خرابکاری** و ایجاد مزاحمت برای کاربران است. برای مثال نمونه‌ای از این دسته از جاسوس‌افزارها به تغییر خودکار صفحه پیش‌فرض مرورگر و یا باز کردن سایت‌هایی که هیچ‌گاه آدرس آنها را تایپ نکرده‌اید، می‌پردازند. همچنین ممکن است نوارابزاری ناخواسته روی مرورگر نصب کنند که معمولا حذف آنها به سادگی میسر نیست.

- گونه دیگری از جاسوس‌افزارها هم وجود دارند که توسط خود کاربران برای اهدافی خاص نصب می‌شوند. از آن جمله می‌توان به keyloggerها اشاره کرد که توسط خود کاربر روی یک کامپیوتر عمومی نصب می‌شود تا کلمات تایپ‌شده توسط کاربری دیگر روی همان کامپیوتر را ثبت و ضبط نماید! هدف از این گونه از جاسوس‌افزارها نیز نوعی **جاسوسی** است.

کاربران معمولا از وجود جاسوس‌افزار مطلع نیستند و این کار شناسایی آنها را سخت‌تر می‌کند.

دلایل وجود جاسوس‌افزار روی سیستم

احتمال آنکه سیستم شما جاسوس‌افزار داشته باشد زیاد است، اما علایم آن چیست؟

۱ـ باز شدن سایت‌هایی که آدرس آنها را تایپ نکرده‌اید
۲ـ باز شدن پیاپی تبلیغات به صورت pop-up
۳ـ نصب خودکار نوارابزار ناخواسته روی مرورگر اینترنت سیستم
۴ـ تغییر ناخواسته صفحه پیش‌فرض مرورگر
۵ـ نتایج اشتباه در جستجو توسط جستجوگر داخلی مرورگر
۶ـ کاهش قابل توجه سرعت کامپیوتر
۷ـ قفل کردن مرورگر و عدم انجام صحیح دکمه‌ها و منوهای آن
۸ـ فعالیت مداوم و سنگین هارددیسک حتی در مواقع بی‌کاری سیستم
۹ـ و هرگونه رفتار مشکوک از برنامه‌ها و به خصوص مرورگرها

پیشگیری از ابتلا به جاسوس‌افزار

همیشه گفته می‌شود پیشگیری بهتر از درمان است. رعایت نکات زیر احتمال آلوده شده سیستم به جاسوس‌افزار را کاهش می‌دهد:

۱ـ همیشه یک نرم‌افزار ضد جاسوس‌افزار که قابلیت آپدیت داشته باشد، روی سیستم داشته باشید.

۲ـ توصیه می‌شود روی لینک‌ها و یا عکس‌های پنجره‌های تبلیغاتی در اینترنت کلیک نکنید. چرا که کلیک روی آنها منجر به نصب جاسوس‌افزار پنهان‌شده در زیر آن می‌گردد. البته تمامی پنجره‌های تبلیغاتی آلوده نیستند، اما بهتر است با عینک بدبینی به آنها بنگرید. این گونه پنجره‌ها را از طریق دکمه Close آنها ببندید.

۳ـ در سایت‌های ناشناس هر سوالی که از شما پرسیده می‌شود را با جواب خیر همراهی کنید. معمولا یکی از مهم‌ترین راه‌های نفوذ جاسوس‌افزار از طریق همین سوال‌هاست. اغلب سوالی از کاربر پرسیده می‌شود و در صورت زدن دکمه yes نرم‌افزار جاسوس‌افزار به صورت خودکار روی سیستم نصب می‌شود.

۴ـ سعی کنید همیشه از سایت‌های معتبر فایل دانلود کنید. بسیاری از سایت‌های مشکوک در پوشش ارایه نرم‌افزارهای کاربردی، اقدام به توزیع جاسوس‌افزار می‌کنند. مثلا شما یک نرم‌افزار پخش موسیقی را دانلود می‌کنید و روی سیستم نصب می‌کنید، غافل از اینکه همراه این نرم‌افزار موسیقی یک جاسوس‌افزار نیز در حال نصب روی سیستم است.

۵ـ ایمیل‌هایی که با عناوین وسوسه‌کننده و جالب دریافت کرده‌اید، اما فرستنده آنها را نمی‌شناسید، باز نکنید. در صورت باز کردن به هیچ عنوان روی لینک‌های آن کلیک نکنید.

۶ـ توصیه‌هایی که از سایت‌های مختلف به شما می‌شود، مبنی بر اینکه سیستم شما ویروسی است، را نادیده بگیرید! این یکی از رایج‌ترین روش‌های نصب جاسوس‌افزار است. بسیاری از سایت‌ها در قالب اسکن کامپیوتر به صورت رایگان، در حال جاسوسی و نصب جاسوس‌افزار روی سیستم شما هستند.

حذف جاسوس‌افزار

به هر حال امکان مبتلا شدن سیستم به جاسوس‌افزار وجود دارد. در این صورت باید به یکی از دو روش زیر اقدام به پاک‌سازی سیستم نمایید:

- استفاده از نرم‌افزارهای تخصصی ضدجاسوس‌افزار مثل Ad-Aware، SpySweeper، Spyware Doctor و ...
- استفاده از ضدویروس‌هایی که قابلیت ضد جاسوس‌افزار هم دارند مثل AVG، Kaspersky، Bitdefender و ...

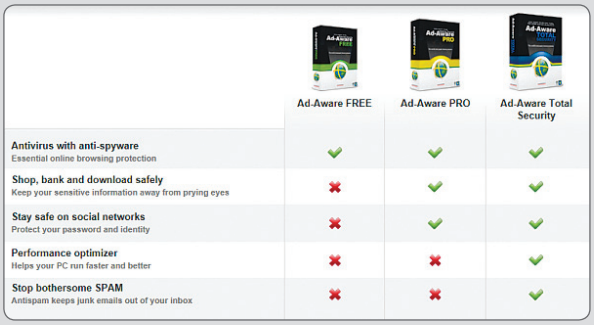
در ادامه به بررسی یکی از محبوب‌ترین نرم‌افزارهای ضد جاسوس‌افزار به نام Ad-Aware می‌پردازیم.

معرفی نرم افزار Ad-Aware

این نرم‌افزار در ۳ نسخه متفاوت عرضه می‌شود: نسخه Free، نسخه Pro و نسخه Total Security.

نسخه Free را می‌توان به صورت رایگان از سایت مربوطه دانلود کرد، اما سایر نسخه‌ها مجانی نبوده و باید خریداری شوند. البته نسخه Pro و Total Security به در دی‌وی‌دی این شماره وجود دارد!

تفاوت این ۳ نسخه در شکل ۱ نشان داده شده است.



شکل ۱: مقایسه نسخه‌های متفاوت Ad-Aware

همانطور که در شکل ۱ می‌بینید، حتی نسخه رایگان Ad-Aware هم می‌تواند به عنوان یک ضد جاسوس‌افزار عمل کند.

در کنار قابلیت کلیدی ضدویروس و ضد جاسوس‌افزار که در تمامی نسخه‌های Ad-Aware وجود دارد، قابلیت‌های دیگری هم به نسخه‌های پولی این نرم‌افزار اضافه شده که بسیار کاربردی هستند. به طور مثال نسخه‌های پولی امکان انجام عملیات خرید اینترنتی و بانکداری اینترنتی را به صورت ایمن تضمین می‌کنند. همانطور که می‌دانید، امروزه بسیاری از خریدها حتی در کشور ما توسط اینترنت انجام می‌شود، از خرید بلیت کنسرت گرفته تا خرید کتاب و نرم‌افزار و ...

خطری که بالقوه هر کاربری را تهدید می‌کند، احتمال لو رفتن مشخصات شماره حساب بانکی وی در حین خرید الکترونیکی است. در واقع جاسوس‌افزارها منتظر چنین شرایطی هستند تا با سرقت اطلاعات کارت شما و ارسال آن به مقصدی نامشخص بتوانند در فرصتی مناسب حساب شما را خالی کنند.

قابلیت مهم دیگر نسخه‌های پولی امکان دانلود ایمن از سایت‌های مختلف است. این نرم‌افزار مانع از دانلود فایل‌هایی می‌شود که همراه خود جاسوس‌افزار دارند.

چون بسیاری از کاربران وقت خود را در شبکه‌های اجتماعی می‌گذرانند و هر روز خبری در مورد لو رفتن اطلاعات خصوصی افراد سرشناس در این شبکه‌ها به گوش می‌رسد، بسیار لازم است توسط نرم‌افزارهایی از این دست مانع از برخی فعالیت‌های جاسوسی شوید. نسخه‌های پولی Ad-Aware تا حد زیادی امنیت اطلاعات خصوصی شما را در شبکه‌های اجتماعی تضمین می‌کند.

نسخه‌های پولی Ad-Aware همچنین امکان افزایش راندمان سیستم را فراهم می‌کنند و با حذف برنامه‌های مزاحم و بهینه‌سازی رجیستری، سرعت کامپیوتر را افزایش می‌دهند.

یکی دیگر از ویژگی‌های نسخه‌های پولی Ad-Aware جلوگیری از ورود ایمیل‌های مشکوک و هرزنامه‌ها به inbox ایمیل شماست. ■

فایروال چیست؟

هومن سیاری
Sayyari@ComputerNews.ir

یکی از ابزارهای مهم امنیتی که نام آن برای اغلب کاربران آشناست فایروال نام دارد. اما فایروال چیست و چه کاری انجام می‌دهد؟

فایروال یک دستگاه سخت‌افزاری یا یک برنامه نرم‌افزاری و یا ترکیبی از سخت‌افزار و نرم‌افزار است که ۲ کار اصلی را انجام می‌دهد:

۱ـ جلوگیری از ورود اطلاعات ناخواسته به کامپیوتر مثل جلوگیری از نفوذ هکرها.

۲ـ جلوگیری از خروج اطلاعات ناخواسته از کامپیوتر مثل جلوگیری از خروج اطلاعات شخصی توسط نرم‌افزارهای جاسوسی.

در واقع فایروال مانند دیواری بین کامپیوتر و دنیای خارج عمل می‌کند و هر گونه ورود و خروجی بین آنها باید از طریق این دیوار و با کنترل و اجازه آن انجام شود.

امروزه تعداد هکرها افزایش پیدا کرده و سلیقه آنها هم تغییر کرده است. تا چند سال پیش تمام فکر و ذکر هکرها نفوذ به مراکز مهم دولتی، تجاری، سیاسی و ... بود اما در حال حاضر آنها به اطلاعات شخصی افراد هم علاقه‌مند شده‌اند و شاید هر کدام از ما حداقل چند نفری را بشناسیم که کامپیوتر، اکانت ایمیل، اکانت شبکه‌های اجتماعی و ... آنها هک شده باشد. وجود یک فایروال می‌تواند درصد بالایی از این حملات را خنثی کند.

از طرف دیگر با رشد روزافزون دانلود انواع نرم‌افزارها و فایل‌های موزیک و فیلم و ... این امکان وجود دارد که یک برنامه جاسوسی (Spyware) به همراه آنها وارد کامپیوتر شده و اقدام به جمع‌آوری و ارسال اطلاعات شخصی شما برای مقصدی نامعلوم نماید. در صورتیکه یک فایروال داشته باشید این نرم‌افزار جاسوسی نمی‌تواند اطلاعات جمع‌آوری‌شده را ارسال نماید و حمله عقیم می‌ماند.

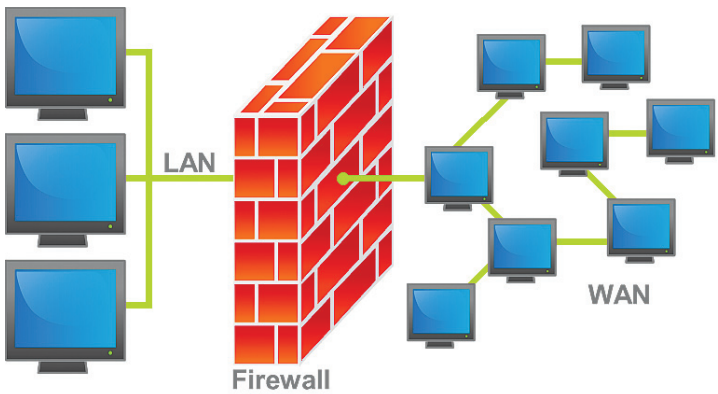
کاربرد دیگر فایروال‌ها در جلوگیری از ارسال اسپم توسط کامپیوتر شماست. بعضی از نرم‌افزارهای جاسوسی و یا ویروس‌ها وارد کامپیوتر شده و پس از دسترسی به لیست کانتکت‌های شما اقدام به ارسال ایمیل‌هایی نامربوط با ایمیل شما برای دوستان و آشنایان و گاهی افراد ناشناس می‌نماید. در حال حاضر یک نمونه از این ویروس در کشور ما به وفور دیده می‌شود. فایروال می‌تواند این مشکل را شناسایی کند و مانع از انجام آن گردد.

کاربرانی که از اینترنت ADSL استفاده می‌کنند از آنجایی که همیشه به اینترنت متصل هستند باید حتما یک فایروال داشته باشند چرا که در غیر اینصورت به هدفی ساده برای هکرها تبدیل می‌شوند.

انواع فایروال

همانگونه که اشاره شد فایروال‌ها به ۲ دسته تقسیم می‌شوند:

۱ـ فایروال‌های سخت‌افزاری: دستگاه‌هایی هستند که معمولا برای حفاظت از داده‌های مجموعه‌ای



شکل ۱: عملکرد فایروال

از کامپیوترهـا در مقابـل نفوذ و جاسوسـی مورد اسـتفاده قـرار می‌گیرنـد. معمـولا بـرای حفظ امنیت شبکه‌های کامپیوتری باید از فایروال‌های سـخت‌افزاری استفاده کرد. هر چه داده‌های یک شبکه کامپیوتری مهم‌تر باشد، اهمیت استفاده از فایروال‌های سـخت‌افزاری قوی‌تر و البته گران‌تر بیشـتر می‌شـود. مثلا مجموعه شـعب یک بانک تشـکیل یک شـبکه را می‌دهد کـه اطلاعات آن بسـیار مهم اسـت و لذا باید از بهترین و قوی‌ترین فایروال‌ها برای جلوگیری از نفوذ هکرها استفاده کرد. از معروفترین فایروال‌های سخت‌افزاری می‌توان به فایروال‌های سخت‌افزاری سیسکو اشاره کرد.

۲ـ فایروال‌هـای نرم‌افزاری: برنامه‌هایی هسـتند که به صورت نرم‌افزاری کلیـه ورود و خروج داده‌ها را بـه و یـا از کامپیوتر کنترل می‌کننـد. اینگونه فایروال‌ها مناسب استفاده‌های شخصی و خانگی و یا شبکه‌های کوچک مثل کافی‌نت‌ها می‌باشد. از معروفتریـن فایروال‌های نرم‌افـزاری می‌توان بـه فایـروال داخلـی ویندوز، ISA Server و Zone Alarm اشاره کرد.

البته در مراکزی که امنیت اطلاعات بسیار بالاست از ترکیب هر دوی این فایروال‌ها استفاده می‌شود.

فایروال‌ها از منظری دیگر به دو گروه تقسیم می‌شوند:

۱ـ فایروال‌هـای یکطرفـه: این دسـته از فایروال‌ها فقـط راه نفوذ به کامپیوتر را می‌بندند و در مقابل ارسـال اطلاعات از کامپیوتر به دنیای خارج هیچ عکس‌العملی از خود نشـان نمی‌دهنـد. فایروال داخلی ویندوز از این گروه است.

۲ـ فایروال‌هـای دوطرفه: این دسـته از فایروال‌ها هم ورود اطلاعـات به کامپیوتر و هم خروج اطلاعات از کامپیوتر را کنترل می‌کنند مثل Zone Alarm.

فایروال به تنهایی کافی نیست

نکته مهمی که باید در اینجا به آن اشاره کرد آن است که فایروال به تنهایی برای حفظ امنیت کامپیوتر شـما کافی نیست. فایروال فقط وظیفه کنترل ورود و خروج اطلاعات به و یا از کامپیوتر را بر عهده دارد اما نمی‌تواند جلوی هجوم ویروس‌ها را بگیرد. از طرف دیگر قادر به از بیـن بردن ویروس‌ها و نرم‌افزارهای جاسوسـی هم نیست. بنابراین باید از فایروال در کنار یک آنتی‌ویروس خوب و یک Anti Spyware استفاده کرد.

فایروال ZoneAlarm

در ادامه به بررسـی یک فایروال قدیمی و توانا به نام ZoneAlarm از شـرکت Check Point می‌پردازیم.

این فایروال در ۴ نسـخه عرضه می‌گردد که تفاوت آنها در قالب شکل زیر نمایش داده شده است.

We offer solutions to fit all of your security needs.	Internet Security Suite	Pro Firewall	Free Firewall
Two-Way Firewall Makes your PC invisible to hackers and stops spyware from sending your data out to the Internet.	✓	✓	✓
Advanced Download Protection Warns you if you try to download a dangerous program.	✓	✓	✗
Support Offers 24/7 live chat and free latest version upgrades.	✓	✓	✗
Antivirus/Antispyware Detects and removes viruses, spyware, Trojan horses, worms, bots, and more.	✓	✗	✗
Parental Controls Filters and blocks inappropriate websites.	✓	✗	✗

برخی از مهم‌ترین ویژگی‌های این نرم‌افزار جالب عبارتست از:

- کنترل ورود اطلاعات به کامپیوتر و عدم اجازه به درخواست‌های ورود مشکوک
- کنترل اطلاعات خروجی از کامپیوتر و عدم اجازه به خروج مشکوک اطلاعات
- ایجاد امنیت در کار با سایت‌های بانکی و یا خرید الکترونیکی
- محافظت در مقابل Keyloggerها
- نظارت بر ترافیک شبکه
- ضد ویروس و ضد نرم‌افزارهای جاسوسی
- حفاظت در مقابل دزدیده شدن اطلاعات شخصی و اکانت‌ها
- حفاظت از ایمیل‌ها
- جلوگیری از ارسال هرزنامه توسط کامپیوتر برای دیگران
- عدم اجازه دسترسی به سایت‌های مشکوک
- بهینه‌سازی سیستم
- حفاظت از داده‌های دیسـک در صورت سرقت نوت‌بوک و یا هارددیسک با رمزگذاری آنها
- تهیه نسخه پشتیبان از اطلاعات به صورت آنلاین
- قابلیت کنترل فرزندان در گشت و گذارهای اینترنتی
- و ...

یکی از قابلیت‌های کاربردی فایروال‌ها در کنترل نرم‌افزارهایی است که می‌خواهند به اینترنت متصل شـوند. حتما شما هم با این مشکل مواجه شده‌اید که نرم‌افزاری را نصـب و کرک کرده‌اید ولی پس از مدتی آن نرم‌افزار از کار افتاده اسـت و دلیل آن اتصـال خـودکار نرم‌افزار مربوطه بـه اینترنت به منظور آپدیت بوده اسـت که سـایت آن نرم‌افزار پس از تشـخیص غیـر اورجینال بودن آن اقـدام به غیر فعال کردنـش نموده اسـت. این مشـکل در مورد بسـیاری از نرم‌افزارهـا مثل Nero، Adobe Photoshop و ... صادق است.

بهترین راه حل برای اینگونه مشـکلات نصب یک فایروال است. در اینصورت اگر نرم‌افزاری بخواهد به اینترنت متصل شود فایروال جلوی آن را گرفته و شما را مطلع می‌کند. در صورتیکه شـما تایید کنید امکان اتصال به اینترنت میسـر می‌شود و در غیر اینصورت از اتصال به اینترنت جلوگیری به عمل خواهد آمد. ■