کامپیوتر و اینترنت
اقتصادی ۲۴
پنجشنبه ۳۱ مرداد ۱۳۸۷ - ۱۹ شعبان ۱۴۲۹ - ۲۱ آگوست ۲۰۰۸ شماره ۲۸۹۲
Thursday, 21Aug 2008, Number 2892

عرضه نخستین گوشی با سیستم عامل گوگل

گوگل اعلام کرد که سیستم عامل جدید آن برای تلفن های همراه که Android نام گرفته است، برای نخستین بار روی یکی از محصولات شرکت HTC(High Tech Computer) نصب و از طریق اپراتور T-Mobile وارد بازار خواهد شد.

به گزارش همکاران سیستم شرکت HTC نیز به منظور رقابت هر چه بیشتر با گوشی iPhone اپل، به این گوشی که یک نمایشگر لمسی بزرگ دارد، یک صفحه کلید کامل اضافه کرده است تا قابلیت های نوشتاری و تایپ کردن در آن آسان تر شود. بر اساس توضیحات گوگل، سیستم عامل Android می تواند گوشی را به ابزار دیجیتالی شخصی برای کاربران تبدیل کند و سرویس ها و ابزارهای مختلف را به صورت جداگانه برای هر کدام از کاربران اجرا نماید.

طراحی کراوات خورشیدی برای شارژ تلفن همراه

گروهی از پژوهشگران دانشگاه دولتی آیووا کراواتی را طراحی کرده اند که با داشتن صفحه های خورشیدی قادر است تلفن همراهی که در آن جای داده می شود را شارژ کند.

به گزارش ایسنا، این پژوهشگران از منسوجات چاپی دیجیتالی برای چاپ پارچه هایی که با الگوی سلول های خورشیدی مطابقت دارند، استفاده کرده اند تا فناوری پوشیدنی بیابند که چندان به چشم نیاید. این کراوات خورشیدی در نور کامل ۳/۶ ولت برق تولید می کند اما بزرگ ترین مشکل این کراوات مهندسی یا ساخت آن نبوده بلکه مربوط به بستن آن است زیرا صفحه های خورشیدی به سادگی تا و خم نمی شوند در نتیجه گره کراوات باید پهن تر از حد معمول باشد.

کارشناسان امنیتی هشدار دادند:

خطر حملات سایبر آمریکا را تهدید می کند

به گفته کارشناسان امنیتی ممکن است حمله نظامی یا تروریستی بزرگ بعدی که علیه آمریکا صورت می گیرد، در فضای سایبر و توسط هکرهایی انجام شود که در آن سوی دنیا قرار دارند.

به گزارش ایسنا، به اعتقاد کارشناسان امنیت اینترنت چنین حمله ای می تواند همچون یک بمباران شدید اثرات ویرانگری بر اقتصاد و زیرساخت آمریکا داشته باشد.

کارشناسان اظهار می کنند که حمله اینترنتی هفته گذشته به جمهوری شوروی سابق گرجستان که پیش از تهاجم نظامی نیروهای روسی آغاز و وب سایت های دولت گرجستان را هدف گرفت، از نوع جدیدی از جنگ سایبر حکایت دارد که آمریکا هنوز برای آن کاملا آماده نشده است.

هکرها حملات هماهنگی علیه سایت های دولت، رسانه ها، بانک ها و حمل و نقل گرجستان انجام دادند؛ در این حملات که به انکار سرویس توزیعی یا داس معروف است، از رایانه های متعددی برای لبریز کردن شبکه ها از میلیون ها تقاضای همزمان، از کار انداختن سرورها و فلج کردن وب سایت ها استفاده شد.

هکرها وب سایت میخاییل شوکایلی، رئیس جمهور گرجستان را بسته و صفحه اول سایت پارلمان این کشور را با قرار دادن تصاویری از آدولف هیتلر و ساکاشویلی که روسیه را برای حمله به این کشور سرزنش می کرد، تغییر دادند.

وب سایت ها و شبکه های رایانه ای دهه هاست که هدف حمله هکرها قرار می گیرند، با این حال حملات سایبر در ابعاد بزرگ و هماهنگ هنوز پدیده نسبتا جدیدی محسوب می شوند.

برخی از کارشناسان امنیت رایانه معتقدند منازعه گرجستان نخستین موردی است که یک حمله سایبر با یک حمله زمینی هم زمان می شود اما به گفته سایرین، حملات رایانه ای مشابهی با عملیات های نظامی در خاورمیانه و سایر نقاط همراه بوده اند.

به گفته تام برلینگ، مدیر اجرایی شرکت میزبان وب Tulip Systems در آتلانتا که داوطلبانه از سرورهای خود برای حمایت از وب سایت های کشور گرجستان در برابر ترافیک های مخرب استفاده کرده، چالش پیش روی کارشناسان امنیتی آمریکا این است که چنین حملاتی می توانند به صورت ناشناس و نسبتا ارزان از هر جای دنیا انجام بگیرند.

هکرهای حمله کننده به گرجستان از شبکه رایانه های آلوده بوت نت یا برنامه های خودکار مخربی استفاده کردند که از روت های شناسایی نشده استفاده کرده و رایانه های هدف خود را با اطلاعات غیرمفید مسدود می کنند.

به گفته کارشناسان امنیت اینترنت، شبکه های رایانه دولت روزانه میلیون ها حملات نفوذی را در آمریکا دفع می کنند؛ وزارت امنیت داخلی آمریکا به منظور هماهنگ سازی دفاع سایبر فدرال و سرعت بخشیدن به پاسخگویی امسال یک مرکز امنیت سایبر ملی را ایجاد کرد.

با این حال گزارش اخیر این وزارتخانه خاطرنشان کرده که هیچ راه موثری برای جلوگیری از یک حمله هماهنگ شده به وب سایت های آمریکا وجود ندارد.

به گفته کارشناسان، از کار انداختن وب سایت های سازمان های امنیتی دولتی کلیدی مانند پنتاگون و سازمان جاسوسی سیا و همچنین شبکه های رایانه ای بانک های بزرگ آمریکایی دشوار است اما یک حمله بزرگ و موفقیت آمیز به سیستم های رایانه ای آمریکا می تواند زیرساخت های حیاتی مانند شبکه های برق رسانی و حمل و نقل را از کار بیندازد.

پژوهشگران فدرال که سال گذشته یک حمله سایبر آزمایشی در آیداهو انجام دادند، خود تخریبی یک ژنراتور را موجب شده و هراس در مورد اثر یک حمله واقعی به شبکه برق رسانی کشور را برانگیختند.

بر اساس یافته های گزارش دفتر نظارت بر حسن عملکرد دولت آمریکا در ماه می، مقامات تنس والی که به حدود ۹ میلیون نفر در جنوب شرقی آمریکا برق فراهم می کنند اقدامات امنیت سایبر کافی به کار نبسته اند.

آنچه که کارشناسان امنیت رایانه را خشمگین می کند این حقیقت است که ویژگی هایی مانند باز بودن و مرتبط بودن که اینترنت را به منبع ارزشمندی تبدیل کرده آسیب رساندن را برای هکرها ساده تر کرده است.

به گفته کارشناسان، حملات سایبر به عنوان جز اصلی جنگ های قرن بیست و یکم به طور فزاینده ای پیشرفته تر شده و دولت ها و صنایع شخصی را وادار خواهند ساخت فایروال های قوی تر و دفاع های دیگری ایجاد کنند.

افزایش سرعت راه اندازی در رایانه ها

فناوری های امروزی با امکانات فراوان، موجب رضایت خاطر کاربران می شوند. فرضا با فشار یک دکمه در دستگاه کنترل از راه دور، تلویزیون را روشن می کنید و یا با فشردن دکمه Start در مایکروفر، دستگاه بلافاصله شروع به کار می کند اما سیستم عامل ویندوز در کامپیوترهای شخصی این گونه نیست و برای راه اندازی آن، بسته به عوامل مختلف باید حدود ۳۰ ثانیه تا چند دقیقه صبر کنید.

البته می توانید از این مدت زمان نسبتا طولانی، برای انجام کار دیگری استفاده کنید اما اگر فرد کم طاقتی هستید، روش هایی برای افزایش سرعت راه اندازی کامپیوتر وجود دارد که برخی از آنها به بهبود عملکرد ویندوز نیز کمک شایانی می کنند. پیش از اعمال این تغییرها ابتدا از سیستم خود، یک نسخه پشتیبان تهیه کنید.

تغییر در برنامه Setup کامپیوتر

ممکن است سخت افزار کامپیوتر شما موجب تاخیر زیادی در راه اندازی ویندوز شود. می توانید با ایجاد تغییراتی اندک در تنظیمات برنامه Setup کامپیوتر، این زمان را کاهش دهید. برای این منظور، مراحل زیر را طی کنید.

ورود به Setup: روش های مختلفی برای انجام این کار وجود دارد اما معمولا با پایین نگهداشتن دکمه Delete یا دکمه ای دیگر به هنگام راه اندازی سیستم، این کار را انجام می دهند. بدین منظور به پیام های ظاهر شده روی صفحه نمایش در هنگام راه اندازی سیستم توجه کرده و یا دفترچه راهنمای مادربرد یا PC خود را مطالعه کنید.

تنظیمات مورد نظر شما، غالبا در زیر گروه ها قرار دارند و نام به کار رفته برای هر تنظیم برحسب سیستم، متفاوت است، از این رو پیام های ظاهر شده را با دقت بخوانید تا گزینه های مربوطه و فرمان های پیمایش مناسب را بیابید. تسریع فرآیند Power On Self-Test آزمایش خودکار به هنگام روشن شدن این گزینه را روی Fast یا Enabled تنظیم کنید تا در هنگام راه اندازی، زمان زیادی به بررسی حافظه و سخت افزار اختصاص نیابد. با انجام این کار تنها مشکل این است که اگر در RAM یا مادربرد، اشکالی باشد، شما متوجه آن نمی شوید.

جست وجوی فلاپی (Floppy Seek): اگر درایو فلاپی کامپیوتر شما به خوبی عمل می کند، لازم نیست در هر بار راه اندازی سیستم، این مسئله بررسی شود. بنابراین آن را در حالت Disabled قرار دهید. درایوهای IDE: به دنبال لیست کانال های اولیه و ثانویه IDE سیستم بگردید. اگر این گزینه ها در حالت Auto قرار داشته باشد، کامپیوتر شما به هنگام راه اندازی، مدت زمانی را صرف شناسایی هر دستگاه IDE می کند. بنابراین بهتر است در کانال های IDE که از آنها استفاده نمی کنید، این گزینه را در حالت None قرار دهید.

بررسی سیستم و حصول اطمینان از عدم حضور ویروس، برنامه های جاسوسی و تبلیغاتی

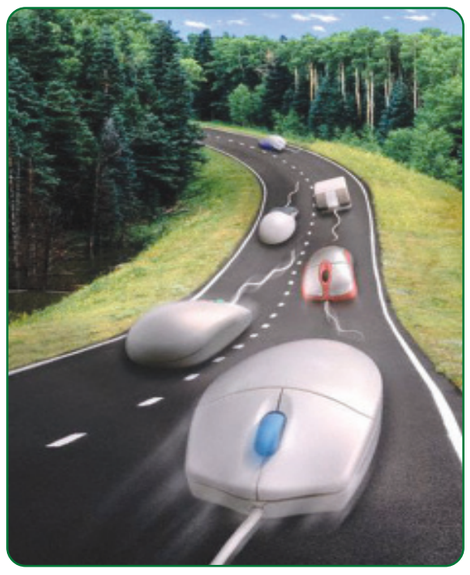
برنامه های پنهانی و زیان آور غالبا در هنگام راه اندازی سیستم بارگذاری می شوند و فرآیند راه اندازی را کند می کنند. با اسکن کردن سیستم، ویروس ها و برنامه های مزاحم را بیابید.

اگر برنامه های ضدویروس و ضدجاسوسی نصب نکرده باشید، با خطرات بسیاری روبه رو خواهید بود. با مراجعه به سایت Trend Microhousecall.trendmicro.com، می توانید به صورت online و رایگان سیستم خود را بررسی کرده و از عدم وجود ویروس اطمینان یابید. برنامه Adaware نیز می تواند در از بین بردن نرم افزارهای جاسوسی و تبلیغاتی به شما کمک کند. همچنین می توانید از برنامه تشخیص دهنده online و رایگان PestScan www.pestscan.com نیز استفاده کنید.

حذف برنامه های غیرضروری

در ویندوز ۹۸، Me و XP می توانید مشاهده کنید که چه برنامه هایی به هنگام راه اندازی بارگذاری می شوند. برای این کار به منوی Start رفته و گزینه Run را انتخاب کنید، سپس عبارت msconfig را تایپ کرده و OK را بزنید. Msconfig در ویندوز ۲۰۰۰ وجود ندارد اما می توانید به جای آن از برنامه هایی مانند Startup Control Panel استفاده کنید.

سپس روی زبانه Start Up کلیک کنید تا فهرستی از برنامه هایی را که به هنگام راه اندازی بارگذاری می شوند، مشاهده کنید. کادرهایی را که در سمت چپ پنجره Msconfig قرار دارند، از حالت علامت دار خارج کنید تا این برنامه ها دیگر بارگذاری نشوند. نام و مکان فایل ها به شما کمک می کند تا عملکرد آن برنامه ها را دریابید.



در ویندوز XP، برنامه Msconfig زبانه ای به نام Services دارد که برنامه های کاربردی دیگر و نیز اجزای سیستم عامل را نشان می دهد. برخی از آنها را می توانید غیرفعال کنید تا به هنگام راه اندازی بارگذاری نشوند اما وجود برخی دیگر برای ویندوز ضروری هستند.

تنظیم رجیستری

برنامه هایی مانند RegClean می توانند تنظیمات سخت افزار و نرم افزارهای منسوخ را از بین ببرند. RegClean برای نسخه های قدیمی ویندوز مناسب است، اما در ویندوز XP می توانید از برنامه های تجاری مانند Norton SystemWorks محصول شرکت Symantec و System Suite محصول شرکت V Communications و اشتراک افزارهایی مانند Registry First Aid استفاده کنید.

یکپارچه سازی هارددیسک

هارددیسک سیستم شما، غالبا فایل ها را فقط در یک مکان ذخیره نمی کند، بلکه بخش های فایل را در هر کجا که فضای خالی باشد، قرار می دهد.

برنامه Disk Defragmenter را در هر یک از درایوهای خود اجرا کنید تا فایل ها به صورت یکپارچه درآیند. این کار، هم موجب بهبود فرآیند راه اندازی و هم عملکرد کلی ویندوز خواهد شد. بدین منظور، به منوی Start رفته و به ترتیب گزینه های Programs,Accessories System Tools و Disk Defragmenter را انتخاب کنید. سپس نام درایو مورد نظر را انتخاب کرده و روی Start کلیک کنید.

parsiforums.com

اثرات کاربرد رایانه بر بینایی کودکان

این روزها میلیونها کودک در سرتاسر جهان از رایانه برای مقاصد آموزشی و تفریحی استفاده می کنند بچه ها نیز مانند بزرگسالان ممکن است در هنگام استفاده از رایانه دچار ناراحتی های چشمی، خستگی، تاری دید و سردرد گردند اما بدلیل ویژگیهای خاص کودکان آنها بیشتر از بزرگسالان مستعد بروز مشکلات ناشی از کار بارایانه هستند.

عوامل بالقوه زیر می توانند بر بینایی کودکان در هنگام استفاده از رایانه تاثیر گذار باشند:

۱- میزان خودآگاهی کودکان بسیار اندک می باشد آنها ممکن است یک کار لذت بخش را با تمرکز زیاد تا مدتها ادامه دهند تا اینکه بالاخره خسته شوند (مانند بازیهای رایانه ای) فعالیت طولانی بدون استراحت کافی می تواند باعث ایجاد مشکلاتی برای سیستم تطابقی چشم و در نتیجه آزردگی آن گردد

مشکلات تطابقی ممکن است بصورت ثابت باقی ماندن توانایی واضح کنندگی چشم در یک فاصله معین و بر روی یک شیی خاص روی دهد در این صورت ممکن است حتی پس از گذشت مدتی از کار اولیه، چشم قادر به تغییر توانایی تطابق خود براحتی و سهولت و برای همه فواصل لازم نباشد علاوه بر این بدلیل عدم جریان کافی اشک بر روی چشم که ناشی از کاهش پلک زدن در هنگام کار با رایانه است چشم دچار آزردگی و ناراحتی می شود.

بالا قرار گرفتن نمایشگر رایانه نیز باعث تشدید این مشکل می گردد بازماندن بیش از حد چشم ها در این حالت باعث تبخیر بیشتر اشک و خشکی و ناراحتی چشم می شود

۲- بچه ها خیلی انعطاف پذیر هستند و این امکان وجود دارد که به مشکلاتی که در اثر استفاده از رایانه برای آنها ممکن است ایجاد گردد عادت نمایند برای مثال کودکی که صفحه نمایشگر رایانه اش بیش از حد روشن است ممکن است هیچگاه به تغییر تنظیمات نمایشگر یا نور محیط برای بدست آوردن شرایط بینایی بهتر فکر نکند در حالیکه این وضعیت (نور زیاد صفحه نمایشگر) می تواند باعث خشکی شدید چشم شود

به همین ترتیب کودکی که دچار تاری دید ناشی از نزدیک بینی، دوربینی یا آستیگماتیسم است ممکن است تصور کند که همه همانطوری می بینند که او می بیند

۳- کودکان هم اندازه بزرگسالان نیستند. از آنجاییکه کودکان کوچک تر از والدین خود هستند بنابراین میزهای کامپیوتری که برای بزرگسالان ساخته شده برای آنها مناسب نیست و بنابراین آنها باید به میزان بیشتری نسبت به بزرگسالان سرشان را بالا بگیرند و این می تواند مشکلاتی را برای کارکرد توام چشمها با یکدیگر برای آنها ایجاد نماید علاوه بر این بچه ها ممکن است برای دسترسی به صفحه کلید ویا چگونگی قرار دادن پاهایشان بر روی زمین مشکلاتی داشته باشند که این خود باعث ایجاد ناراحتی در بازو، گردن و یا پشت بچه ها می گردد

۴- محیط کار بچه ها در خانه یا مدرسه اغلب فاقد نور مناسب می باشد. روشنایی لازم برای استفاده مناسب از رایانه نصف میزان نوری است که در یک کلاس موجود می باشد نور بیش از حد می تواند باعث اذیت شدید چشم ها گردد

برای کودکی که مایل به استفاده از رایانه است به نکات زیر توجه فرمایید:

۱- چشمان کودک را در فواصل معین مورد معاینه بینایی سنجی قرار دهید در صورت نیاز به عینک، لنز تماسی یا هر درمان دیگر استفاده مداوم از آنرا به کودک توصیه نمایید

۲- زمان استفاده از رایانه را قویا برای کودک محدود نمایید برای هر یک ساعت استفاده پیوسته از رایانه حداقل ده دقیقه استراحت لازم است

۳-ارتفاع و سایر تنظیمات رایانه بدقت کنترل نمایید اندازه و قد کودک جایگاه نمایشگر و صفحه کلید را مشخص می نماید در بسیاری موارد نمایشگر خیلی بالا قرار دارد، صندلی خیلی کوتاه است و یا میز خیلی بلندتر از حد مورد نیاز برای کودک می باشد چاره بسیاری از مشکلات این چنینی استفاده از صندلی های دارای قابلیت تنظیم ارتفاع می باشد زیرا تغییر جایگاه نمایشگر همیشه امکانپذیر نیست

۴- میزان درخشندگی صفحه نمایشگر را بخوبی تنظیم نمایید

۵-میزان نور اتاق را کاهش دهید تاهم اندازه روشنایی صفحه نمایشگر رایانه گردد.

برای کار راحت با رایانه، کودکان به شرایطی متفاوت از بزرگسالان نیاز دارند. با کمی تلاش می توان از مطلوب بودن شرایط برای استفاده کودکان از رایانه اطمینان حاصل نمود و عادات خوب بینایی را در آنان تقویت نمود.

setaregan.net

پویش پورت ها

پویش یک پورت فرآیندی است که مهاجمان با استفاده از آن قادر به تشخیص وضعیت یک پورت بر روی یک سیستم و یا شبکه می باشند. مهاجمان با استفاده از ابزارهای متفاوت، اقدام به ارسال داده به پورت های TCP و UDP نموده و با توجه به پاسخ دریافتی قادر به تشخیص این موضوع خواهند بود که کدام پورت ها در حال استفاده بوده و از کدام پورت ها استفاده نمی گردد و اصطلاحاً آنان باز می باشند. مهاجمان در ادامه و بر اساس اطلاعات دریافتی، بر روی پورت های باز متمرکز شده و حملات خود را بر اساس آنان سازماندهی می نمایند. عملکرد مهاجمان در این رابطه مشابه سارقانی است که به منظور نیل به اهداف مخرب خود (سرقت)، درابتدا وضعیت درب ها و پنجره های منازل را بررسی نموده تا پس از آگاهی از وضعیت آنان (باز بودن و یا قفل بودن)، سرقت خود را برنامه ریزی نمایند.

Transmission Control Protocol(TCP) و User Datagram Protocol (UDP)، دو پروتکل مهم TCP/IP می باشند. هر یک از پروتکل های فوق می توانند دارای شماره پورتی بین صفر تا ۶۵,۵۳۵ باشند. بنابراین ما دارای بیش از ۶۵۰۰۰ درب می باشیم که می بایست در رابطه با باز بودن و یا بستن هر یک از آنان تعیین تکلیف نمود (شبکه ای با بیش از ۶۵۰۰۰ درب!). از ۱۰۲۴ پورت اول TCP به منظور ارائه سرویس های استانداردی نظیر FTP,HTTP,SMTP و DNS استفاده می گردد. (پورت های خوش نام). به برخی از پورت های بالای ۱۰۲۳ نیز سرویس های شناخته شده ای نسبت داده شده است، ولی اغلب این پورت ها به منظور استفاده توسط یک برنامه در دسترس می باشند.

نحوه عملکرد برنامه های پویش پورت ها

برنامه های پویش پورت ها در ابتدا اقدام به ارسال یک درخواست برای کامپیوتر هدف و بر روی هر یک از پورت ها نموده و در ادامه با توجه به نتایج بدست آمده، قادر به تشخیص وضعیت یک پورت می باشند (باز بودن و یا بسته بودن یک پورت). در صورتی که اینگونه برنامه ها با اهداف مخرب به خدمت گرفته شوند، مهاجمان قادر به تشخیص وضعیت پورت ها بر روی یک سیستم و یا شبکه کامپیوتری می شوند. آنان می توانند تهاجم خود را بگونه ای برنامه ریزی نمایند که ناشناخته باقی مانده و امکان تشخیص آنان وجود نداشته باشد. برنامه های امنیتی نصب شده بر روی یک شبکه کامپیوتری می بایست بگونه ای پیکربندی شوند که در صورت تشخیص ایجاد یک ارتباط و پویش مستمر و بدون وقفه مجموعه ای از پورت ها در یک محدوده زمانی خاص توسط یک کامپیوتر، هشدارهای لازم را در اختیار مدیریت سیستم قرار دهند. مهاجمان به منظور پویش پورت ها از دو روش عمده «آشکار» و یا «مخفی»، استفاده می نمایند. در روش پویش آشکار، مهاجمان در رابطه با تعداد پورت هائی که قصد بررسی آنان را دارند، دارای محدودیت خواهند بود (امکان پویش همه ۶۵,۵۳۵ پورت وجود ندارد). در پویش مخفی، مهاجمان از روش هائی نظیر «پویش کند» استفاده نموده تا احتمال شناسائی آنان کاهش یابد. با پویش پورت ها در یک محدوده زمانی بیشتر، احتمال تشخیص آنان توسط برنامه های امنیتی نصب شده در یک شبکه کامپیوتری کاهش پیدا می نماید.

برنامه های پویش پورت ها با تنظیم فلاگ های متفاوت TCP و یا ارسال انواع متفاوتی از بسته های اطلاعاتی TCP قادر به ایجاد نتایج متفاوت و تشخیص پورت های باز بر اساس روش های مختلفی می باشند. مثلاً یک پویش مبتنی بر SYN با توجه به نتایج بدست آمده اعلام می نماید که کدام پورت باز و یا کدام پورت بسته است و یا در یک پویش مبتنی بر FIN بر اساس پاسخی که از پورت های بسته دریافت می نماید (پورت های باز پاسخی را ارسال نخواهند کرد) وضعیت یک پورت را تشخیص خواهد داد.

چگونگی پیشگیری و حفاظت

مدیران شبکه می توانند با استفاده از امکانات متنوعی که در این رابطه وجود دارد از پویش پورت ها بر روی شبکه توسط مهاجمان آگاه گردند. مثلاً می توان همه پویش های مبتنی بر SYN را ثبت تا در ادامه امکان بررسی دقیق آنان وجود داشته باشد. (تشخیص ارسال یک بسته اطلاعاتی SYN به پورت های باز و یا بسته).

به منظور افزایش ایمن سازی کامپیوتر و یا شبکه مورد نظر می توان خود راسا اقدام به پویش پورت ها نمود. با استفاده از نرم افزارهائی نظیر NMap می توان محدوده ای از آدرس های IP و پورت های مورد نظر را بررسی نمود (شبیه سازی یک تهاجم).

پس از مشخص شدن وضعیت هر یک از پورت ها می بایست اقدامات لازم حفاظتی در این خصوص را انجام داد. در صورتی که به وجود (باز بودن) یک پورت نیاز نمی باشد، می بایست آنان را غیر فعال نمود. در صورت ضرورت استفاده از یک پورت، می بایست بررسی لازم در خصوص تهدیداتی که ممکن است از جانب آن پورت متوجه سیستم و یا شبکه گردد را انجام و با نصب patch های مرتبط با آنان امکان سوءاستفاده از پورت های باز را کاهش داد.

srco.ir