راهنمایی برای امنیت رایانه‌های خانگی

نوشته: باب ماهان ـ ترجمه: محمدحسن دزیانی

این متن از برنامه طبقه‌بندی نشده امنیت کامپیوتر در لابراتوار ملی شمال‌غرب پاسیفیک انتخاب شده است(ww.pnl.gov/) . دسامبر ۲۰۰۳

■ نگاه مختصر

این راهنما اطلاعاتی برای کمک به حفاظت از کامپیوتر خانگی شما از حملات و دیگر حوادثی ارائه می‌کند که می‌تواند سیستم شما یا اطلاعات ذخیره شده روی آن را آسیب برساند.

اگر از کامپیوتر در خانه استفاده می‌کنید، به اینترنت دسترسی دارید و به طور مداوم از تدابیر حمایتی استفاده نمی‌کنید، از خطرات ویروس‌ها، کرم‌ها و هکرها آگاه شوید. به‌هرحال، آگاهی از تهدید کمک زیادی به شما نمی‌کند، اگر نخواهید برای خنثی کردن خطر کاری کنید. دقت کنید، گام‌هایی وجود دارد که می‌توانید برای کاهش احتمال موفقیت یک حمله استفاده کنید.

چهار شرط، لازمه یک حمله موفقیت‌آمیز است خواه ناشی از ویروس، کرم یا هکر باشد.

۱- اولاً باید تهدیدی وجود داشته باشد. غالباً آگاهیم که تهدیدات واقعی هستند. ویروس، کرم‌ها و هکرها انواع تهدیدهایی هستند که درباره آن‌ها مطالبی خوانده‌ایم یا تجربه کرده‌ایم.

۲- ثانیاً کامپیوتر شما باید در برابر یک تهدید آسیب‌پذیر باشد. باوجود تنوع و رشد تولید و فارغ از روشن بودن سیستم یا خیر، همه سیستم‌های کامپیوتری آسیب‌پذیرند. یکی از مهم‌ترین آسیب‌پذیری‌ها خود کاربر است. هر زمان شما دانلود و برنامه‌ای را اجرا می‌کنید یا یک فایل ضمیمه ایمیل را باز می‌کنید، شما خطر دانلود کردن یک برنامه مضر را می‌پذیرید. هم‌چنین آسیب‌پذیری، نرم‌افزار را در کامپیوتر شما تحت تأثیر قرار می‌دهد، هنگامی که امنیت آن ضعیف باشد.

۳- ثالثاً، باید کوششی جهت اکتشاف آسیب‌پذیری صورت گیرد. این اکتشاف یک حمله است که از آسیب‌پذیری برای ورود و به کارگیری (توأم با سازگاری با) سیستم شما استفاده می‌کند. اکتشافات می‌توانند ساده یا پیچیده باشند. یک مثال از اکتشاف ساده ارسال ویروس ضمیمه شده بر یک ایمیل است. اگر شما ضمیمه را باز کنید، کامپیوتر شما ممکن است آلوده شود.

۴- سرانجام، کامپیوتر شما باید هدف و آماج قرار گرفته باشد و کوششی برای اکتشاف آسیب‌پذیری به خاطر بکارگیری و سازگاری با کامپیوتر شما شده باشد. این نوعاً یک موضوع احتمالات است. هرچه کامپیوتر شما با اینترنت بیشتر سروکار داشته باشد، احتمال بیشتری وجود دارد که کامپیوتر شما هدف قرار گیرد (مثلاً برای ویروس) و کوششی برای اکتشاف صورت گیرد.

خبر بد اینکه نمی‌توانید خطر را از کامپیوتر خود دور کنید. هیچ چیزی به عنوان امنیت مطلوب کامپیوتر وجود ندارد. خبر خوب این که می‌توانید بطور قابل توجهی این احتمال را کاهش دهید که سیستم شما برای حمله مورد استفاده قرار گیرد.

■ ارتباطات اینترنتی

ارتباطات اینترنتی مجرای اصلی برای حملات رسیدن به کامپیوتر شما می‌باشد. ارتباطات اینترنتی به دو شکل عمده قابل دسترسی هستند: شماره‌گیری با سرعت پایین و دستیابی با سرعت بالا. بسیاری کاربران کامپیوتر خانگی با استفاده از مودمی از اینترنت استفاده می‌کنند که به سروری از طریق خط تلفن متصل می‌شود. سرور توسط ISP ارائه و تأمین می‌شود (مانند مخابرات One World یا آمریکا آن لاین). زمان اتصال، شما از امکانات سرور برای جستجو در اینترنت استفاده می‌کنید.

اخیراً دستیابی با سرعت بالا در بیشتر زمینه‌ها و حوزه‌ها از جمله Tri-Cities قابل دسترس شده‌اند. دستیابی با سرعت بالا شامل موارد زیر است:

- دستیابی مودم کابلی از یک تهیه‌کننده خدمات تلویزیون کابلی محلی
- خطوط مشترک کننده دیجیتال (DSL) از یک شرکت تلفن
- دستیابی بی‌سیم از یک تهیه‌کننده خدمات بی‌سیم
- ماهواره

این خدمات با سرعت بالا غالباً تحت عنوان ارتباطات پیوسته (always on connection) شناخته شده‌اند زیرا در همه اوقات قابل دسترس هستند. دسترسی با سرعت بالا چند مزیت دارد:

– صفحات وب سریع‌تر دریافت و مشاهده می‌شود. این امر زمان نصب برنامه، روزآمد کردن آن، دریافت تصاویر یا دیگر فایل‌های بزرگ خیلی قابل مشاهده است.

– به جز اوقاتی که سرویس برای نگهداری و کنترل کند می‌شود، ارتباط غالباً میسر است. هیچ شماره تلفنی برای شماره‌گیری و هیچ سیگنال مشغولی وجود ندارد.

– ارتباط تلفنی شما را بلوکه نمی‌کند. ارتباطات کابلی، ماهواره‌ای و بی‌سیم جدای از تلفن شما هستند. DSL خط تلفن شما را بین تماس‌های تلفنی (صوتی) و سرویس اینترنت بدون هیچ تعارضی به اشتراک می‌گذارد.

■ خطرات

هر زمانی شما آن لاین هستید، سیستم شما میت‌واند توسط کرم یا ویروس آلوده شود، ندانسته به یک وب سایت مضر وارد شوید، یا مستقیماً توسط یک هکر مورد حمله قرار گیرید. ویروس‌ها نوعاً توسط برخی اعمال شما نظیر لود کردن یک دیسک آلوده یا باز کردن یک ضمیمه پست الکترونیک که آلوده باشد، وارد سیستم می‌شوند. کرم‌ها موذی‌تر هستند. کرم‌ها مستقیماً از عمل شما ناشی نمی‌شوند. آن‌ها از شبکه بدون کمک و به تنهایی وارد سیستم شما شده آن را آلوده می‌کنند. هم کرم‌ها و هم هکرها سیستم شما را از طریق استفاده از آدرس اینترنتی سیستم شما هدف قرار می‌دهند.

زمانی شما به اینترنت متصل می‌شوید، به واسطه یک آدرس اینترنتی مشتمل از اعداد منحصر به فرد شناسایی شده و دارای هویت می‌شوید. در ارتباطات از طریق شماره‌گیری، وضعیت متفاوتی پیش می‌آید هر زمان که به ISP خود لاگ می‌کند. به علت این که آدرس شما تنها زمانی که آن لاین هستید معتبر است، خطر مورد حمله قرار گرفتن توسط هکرها ضعیف است اگرچه صفر نیست (یعنی تا هر مدت آن لاین باشید می‌توانید مورد حمله قرار گیرید).

وضعیت در دستیابی با سرعت بالا متفاوت است. آدرس اینترنتی شما در طول یک دوره طولانی (روزها یا هفته‌ها) بدون تغییر می‌ماند برعکس روش شماره‌گیری که با هر بار دستیابی این آدرس تغییر می‌کند. همچنین دائماً کامپیوتر شما متصل به اینترنت است مگر این که آن را خاموش کنید یا واسط دستیابی را قطع ارتباط کنید (مثلاً کابل مودم را قطع کنید).

اگر کامپیوتر روشن است و متصل به اینترنت، پس می‌تواند مورد حمله قرار گیرد زیرا هکرها دائماً اینترنت را برای آدرس‌هایی جهت حمله اسکن می‌کنند. همچنین هکرها مایل به ورود به کامپیوترهایی هستند که از سرعت بالای ارتباط اینترنتی بهره می‌برند. مثلاً، یک عضو لاباتوار ملی شمال غرب پاسیفیک با یک سرویس با سرعت بالا، دیواره آتش Black ICE را روی کامپیوتر خانه‌اش نصب کرده و آن را در طول شب روشن گذاشته است. بالغ بر ۵۰ بار در طول یک ساعت برای دستیابی و سوءاستفاده (حمله اکتشافی) کامپیوتر او، حمله صورت گرفته است. این سطح از فعالیت برای سیستم‌های استفاده کننده از دستیابی با سرعت بالا غیرمعمول نیست. خوشبختانه، هیچ کدام از حملات موفقیت‌آمیز نبود.

■ کاهش خطر

می‌توانید با اتخاذ چند رویه به طور جالب توجهی خطر مواجهه با کد مضر یا رهایی سیستم کامپیوتری‌تان را در صورتی که مورد حمله قرار گرفته باشد، کاهش دهید.

۱ – نرم‌افزار ضد ویروس:

نرم‌افزار ضد ویروس (AV) سیستم را برای حضور نرم‌افزار مضر پویش می‌کند. آن سیستم حافظه و فایل‌های دیسک را پویش می‌کند و به طور اتوماتیک به گونه‌ای پیکربندی شده که هر فایل را که در حال باز شدن روی سیستم شما باشد، پویش کند. این ویژه برای ضمایم ایمیل مفید است. اگر ویروسی کشف شود، نرم‌افزار ضد ویروس برنامه مهاجم را قرنطینه می‌کند یا بر می‌دارد. نرم‌افزار ضد ویروس از یک پایگاه داده حاوی ویروس‌های شناخته شده برای کشف برنامه مهاجم استفاده می‌کند. مطمئن شوید که پیکربندی برنامه ضد ویروس به گونه‌ای است که قادر به بررسی کلیه فایل‌ها قبل از باز شدن باشد. شناخته‌ترین برنامه‌های ضد ویروس شامل ضدویروس نورتون و مک آفی است.

۲ – روزآمد کردن منظم و مرتب ضد ویروس:

به علت این که ویروس‌های جدید به گسترش و رها شدن و توسعه خود ادامه می‌دهند، فایل‌های مربوط باید روزآمد شود. شما باید برنامه ضد ویروس خود را به طور اتوماتیک برای روزآمد شدن در برابر ویروس‌ها تنظیم یا به سایت مربوط برای آخرین روزآمد شدن‌ها مراجعه کنید.

۳ – یک دیواره آتش نصب و استفاده کنید:

دیواره آتش دستیابی به سیستم شما را از طریق اینترنت را محدود می‌کند. این برنامه می‌تواند دستیابی داخلی یا خارجی یا هر دو را محدود کند. این برنامه به شما اجازه می‌دهد که تعیین کنید چه چیز مجاز و کدام غیرمجاز است. دیواره آتش می‌تواند در نرم‌افزار یا سخت‌افزار اجرا شود. دیواره‌های آتش نرم‌افزار روی کامپیوتر شما نصب می‌شوند.

سیستم‌های عامل جدید دارای دیوار آتش در درون خود هستند و دیواره آتش‌های نرم‌افزاری ارزان (مثلاً BlackICE و Zone alarm) نیز برای سیستم‌های عامل قبلی (قدیم‌تر) در دسترس هستند. دیواره‌های آتش سخت‌افزار بین پورت دستیابی شبکه کامپیوتر شما و مودم دستیابی سرعت بالا ارتباط ایجاد می‌کنند (مثلاً کابل یا مودم Ds۲). دیواره‌های آتش سخت‌افزاری از چند ارائه‌کننده و فروشنده با قیمت زیر ۱۰۰ دلار قابل تهیه هستند. همچنین نوعاً این واسط‌ها به عنوان روترهایی کار می‌کنند که به شما اجازه اتصال چند کامپیوتر خانگی را به اینترنت می‌دهد.

۴ – از رویه‌های ایمن برای ایمیل و وب استفاده کنید:

بیشتر و البته نه همه، آلودگی‌ها ویروسی از طریق پست الکترونیک منتقل می‌شوند. یک ویروس غالباً به عنوان یک فایل ضمیمه ارسالی توسط یک دوست یا آشنا دریافت می‌شوند اما می‌تواند از هر منبعی ناشی و ارسال شود. به نرم‌افزار ضدویروس خود به صورت صددرصد کامل اکتفا و اعتماد نکنید.

ویروس‌ها و برنامه‌های کرم جدید هر روز گسترش می‌یابند و رها می‌شوند. فایل ضد ویروس شما ممکن است این منبع ویروسی جدید را نشناسد. اگر ایمیل مشکوکی دریافت کردید، اگرچه از کسی که او را خوب می‌شناسید، آن را باز نکنید و فوراً پاک کنید. همچنین وب سرور ممکن است به طور بی‌سروصدا و حتی ناآگاهانه کدهای مضر را روی کامپیوتر شما دانلود کنند. برای مثال، وب سرورها غالباً صفحات وب را با کد مخفی و محرمانه ارائه می‌کنند زمانی آن صفحه را دانلود می‌کنید. در بیشتر مواقع، کد عملکرد مثبتی دارد (مثلاً اجرای نمایش و تصویر). به هرحال، کد مخفی در برخی صفحات از نوع مضر است و برای آلوده کردن سیستم شما استفاده می‌شود. در حالی که نمی‌توانید غالباً از این امر آگاه باشید که کدام وب سایت میزبان فعالیت مضر است اما می‌توانید در انتخاب سایت‌ها برای دیدن (آن سایت) دقت کنید.

اگر در خانه از کامپیوتر استفاده می‌کنید و به اینترنت دسترسی دارید و به طور مداوم از تدابیر حمایتی استفاده نمی‌کنید از خطرات ویروس‌ها، کرم‌ها و هکرها آگاه شوید

۵ – روزآمد کردن اجزاء و قطعات:

همه نرم‌افزارها، آسیب‌پذیری‌هایی دارند که می‌تواند کشف و مورد استفاده قرار گیرد. همان طور که آسیب‌پذیری‌ها کشف می‌شوند، راه‌های سوءاستفاده غالباً نوشته و برای استفاده همگانی روی اینترنت منتشر می‌شوند.

سازندگان برنامه روی سیستم شما مواردی ←

را در برنامه لحاظ می کنند تا یک آسیب پذیری خاص نتواند از سیستم شما سوءاستفاده کنند همین موارد توسط سازندگان برای کاربران به طور رایگان توزیع می شوند. در برخی موارد، ابزارهای اتوماتیک برای آگاهی کاربران از آسیب پذیری ها و اجزاء مورد نیاز برای دانلود و نصب اتوماتیک در دسترس می باشد. در دیگر موارد، شما نیازمند رجوع به وب سایت فروشنده برنامه برای دریافت ابزار لازم هستید. اجزاء مربوطه و ضدویروس ها معمولاً از طرق مختلف روزآمد نگاه داشته می شوند تا بتوانید از سیستم خود در برابر حملات و آلودگی ها حفاظت کنید.

بالغ بر ۹۰ درصد نفوذهای موفق ناشی از سوءاستفاده از آسیب پذیری های شناخته شده و . . . است. در گذشته، ارائه ابزار روزآمد کردن، هشدار و . . . نیازمند وجود یک متخصص جدا نبود. آگاهی از روش کار ابزارها نیز برای شما سخت بود. اما حالا سیستم های عامل جدیدتر دارای پروسه سودمند و آسان برای همه کاربران از کاربران مبتدی تا پیشرفته هستند. خیلی زیاد توصیه شده که از این امکان و توانایی استفاده کنید حتی اگر این کار مستلزم ارتقاء سیستم عامل شما باشد.

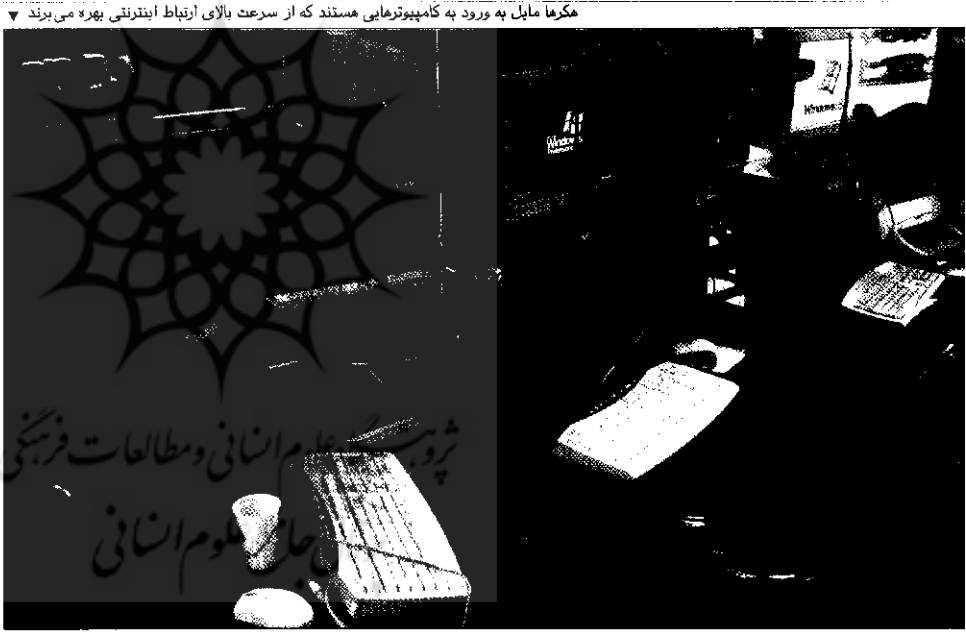
۶- خردمندانه گذرواژه ها را ایجاد و استفاده کنید:

احتمالاً گذر واژه های متنوعی برای دستیابی به کامپیوتر خانگی و سایت های مختلف (مثل بانک، اتحادیه اعتباری، پلان های سرمایه گذاری و . . . مرتبط با شما) که دیدار می کنید، درست می کنید تا حدس زدن و شکستن آن ها سخت تر و پیچیده تر شود. مشکل این است که ممکن است به خوبی و به درستی توانایی به خاطر آوردن همه گذرواژه ها را نداشته باشید اگر آن ها خیلی پیچیده باشند. تبعاً آن ها را جایی می نویسید یا در کامپیوتر خود ذخیره می کنید یا از سیستم یادآوری راه دور استفاده می کنید تا از ورود مجدد آن ها پرهیز کنید. هیچکدام از این ها، ایده خوبی نیست مخصوصاً زمانی اطلاعات خصوصی ای حفاظت می کنید که می توانند در صورت افشا ضرر غیرقابل قبول اجتماعی یا مالی به دنبال داشته باشد. بنابراین، گذرواژه ها باید حفاظت شوند.

۷- از کامپیوتر، پشتیبان (back up) تهیه کنید:

حداقل، باید نسخه پشتیبان از هر گونه اطلاعات مهمی تهیه کنید که روی کامپیوتر ذخیره می کنید. راه های مختلفی برای گرفتن پشتیبان وجود دارد از جمله استفاده از نوارها و درایوهای رایت سی دی. با کاهش هزینه دیسک های ذخیره، می توانید از یک هارد دوم با گنجایش بالا برای گرفتن پشتیبان از همه سیستم یا فقط فایل های مهم خود استفاده کنید. درایوهای USB انتخاب دیگر هستند. اگر یک دیسک اضطراری روی سیستم خود ایجاد نکرده اید، فوراً این کار را انجام دهید.

هکرها مایل به ورود به کامپیوترهایی هستند که از سرعت بالای ارتباط اینترنتی بهره می برند ▼



این دیسک می تواند به شما کمک کند زمانی سیستم اصلی شما بالا نمی آید (boot up). این یک بخش حیاتی در جعبه ابزار شما است.

۸- ویژگی هایی که نیاز ندارید غیرفعال کنید:

کامپیوترها یک سری تنظیم های پیش فرض را ارائه می کنند. تنظیم های متنوعی برای همه چیز از تنظیم رنگ ها گرفته تا حفاظت ایمنی وجود دارند. در گذشته، در بیشتر کامپیوترها تنظیمات امنیتی با پیش فرض «هیچ» (None) ارائه شده و با سرویس هایی نظیر اشتراک پرینتر فعال می شد. دلیل این کار نیز سهولت استفاده از ماشین برای کاربر و ارائه همه سرویس های مورد نیاز او بود. برخی از این سرویس ها مورد استفاده هکرها قرار می گیرد. مثلاً، اشتراک گذاری فایل و پرینت را غیرفعال کنید تا زمانی که به آن نیاز پیدا می کنید یا از آن ها با استفاده از یک دیواره آتش استفاده کنید (آن ها را پشت دیواره آتش بگذارید). خوشبختانه، فروشندگان پیش فرض ها را برای امنیت بیشتر و ایجاد سیستم هایی با حفاظت بیشتر تنظیم می کنند. این یک دلیل دیگر برای ارتقاء (Up grade) سیستم عامل شما است.

۹- ذاتاً از سرویس ها و نرم افزارهای فاقد ایمنی اجتناب کنید:

برخی نرم افزارها و سرویس ها خیلی مورد علاقه کاربران خانگی هستند. نرم افزارهای رایگان، پیام فوری و نرم افزار دانلود موزیک به عنوان محصولات یا سرویس هایی تلقی می شوند که وسیعاً روی کامپیوترهای خانگی استفاده می شوند. نرم افزار رایگان گاه، نرم افزار بزرگی است و گاه نیست.

برخی نرم افزارهای رایگان، با نرم افزارهای تبلیغاتی یا نرم افزارهای جاسوسی توأم هستند که به محض رفتن به فضای سایبر شروع به ارسال گزارش به برخی سایت ها و هکرها و . . . می کنند. شما می توانید تعیین کنید سیستم شما چنین نرم افزارهایی را دریافت کند یا نکند، و از آن جا که این نرم افزارها بدون آگاهی شما نصب می شوند می توانید از سایت www.lavasoftusa.com دیدار و بسته های نرم افزاری رایگان موسوم به Ad-ware را نصب کنید. این بسته ها سیستم شما را برای حضور نرم افزارهای تبلیغاتی و جاسوسی پویش کرده آن را به شما گزارش می کند. این بسته ها برداشتن سیستم های تهاجمی را از سیستم تان پیشنهاد خواهند کرد. پیام فوری اغلب مورد استفاده قرار می گیرد زیرا آن سیستم شما را به روی شخص دیگری که با او صحبت می کنید باز می کند. به یاد داشته باشید فرد ممکن است ناتوان باشد و نیز باید دقیق باشید که از این سرویس برای صرف ارتباط با دیگر افرادی که می شناسید و به آن ها اطمینان دارید، استفاده کنید.

پیام فوری و بسیاری از سرویس های موزیک پاپ هر دو یک شکل از نرم افزار موسوم به نرم افزار peer-to-peer هستند. تعداد زیادی سرویس های دانلود فایل از جمله KaZaA، Morpheus و Bear Share وجود دارد. در هر مورد، شما یک برنامه را روی کامپیوتر خود لود و نصب می کنید. اگر شما نرم افزار را دانلود کنید مطمئن باشید که کنترل شما بر آن برنامه حداقل یا حتی صفر است. یکی از این نرم افزارها به گونه ای تدوین شده که پس از نصب عملیات کامپیوتر شما را در کنترل خود می گیرد و آن را برای مقاصد دیگر استفاده می نند. این به معنای برنامه اسب تروا است. برنامه ای که برای اجرای عملکردهای مشروع ظاهر می شود اما تعداد عملکردهای ناخواسته و غیرمطلوب ناشناخته برای کاربر را نیز انجام می دهد.

سرویس های توزیع فایل همچون کازا، موجب می شود کامپیوتر شما تبدیل به یک سرور شود و دستیابی از اینترنت به کامپیوتر شما توسط دیگر شرکت کنندگان در این شبکه اشتراک فایل مجاز شود. بسته به سرویس، شما می توانید از این کار جلوگیری کنید. اگر شما قصد این ممانعت را ندارید پس اجازه دستیابی به سیستم خود از اینترنت را داده اید و همه خطرات ناشی از آن را پذیرفته اید. همچنین شما می توانید به نقض کپی رایت موزیک خاتمه دهید.

نرم افزار peer-to-peer یک تکنولوژی مورد علاقه دیگران است و بالقوه موارد استفاده مفید و سودمندی دارد. به هر حال، هر پیشرفتی، خطراتی نیز به دنبال دارد و حتی می تواند منجر به فقدان حفاظت سیستم شما شود. بیشتر این تکنولوژی ها فاقد حمایت امنیتی است و نیازمند هیچ تائید یا تصدیق برای شناسایی طرفین و دورنگاه داشتن آن ها از افراد بد نیست. همان طور که خاطرنشان کردیم، دقیق و محتاط باشید اگر از این نرم افزارها استفاده می کنید.

۱۰ - اطلاعات حساس را روی کامپیوتر خود ذخیره نکنید:

اگر کامپیوتر شما هنگ شود، تمام محتوای سیستم توسط حمله کنندگان مورد استفاده قرار می گیرد. پس جستجو و بهره بردن از گذرواژه ها، کلیدهای رمزنگاری، شماره های کارت اعتباری، شماره های تأمین اجتماعی، یا دیگر اطلاعات خصوصی کار آسانی است. بهترین راه عدم ذخیره اطلاعات حساس روی سیستم است. اگر سوابق مالی یا دیگر اطلاعات شخصی را روی کامپیوتر خانگی خود نگه می دارید باید فایل ها را به صورت آف لاین (مثلاً روی یک سی دی) یا به صورت آن لاین به شکل رمزنگاری شده ذخیره کنید. عموماً سیستم های عامل جدید امکانات رمزنگاری قوی ارائه می کنند به گونه ای که می توانید از فایل های مهم حفاظت کنید. این توانایی نیز دلیل دیگری برای ارتقاء سیستم عامل است.

■ منابع

امیدواریم راهنما را مفید یافته باشید و تمام یا بخشی از توصیه های آن را به کار گیرید. اگر نیاز به اطلاعات بیشتر دارید منابع عالی زیر را در وب سایت های ذکر شده تهیه کنید:

■ درباره کابل مودم/ DSL

Cable-dsl.home.att.net/#security

این سایت مطالب مفیدی به صورت مشاوره گام به گام با حمایت شرکت AT&T در اختیار شما می گذارد. خواه سیستم شما مکینتاش باشد خواه ویندوز. همچنین دربارهٔ دیواره آتش خانگی، حریم خصوصی اینترنت، فیلترینگ محتوا برای کودکان، آماده کردن سیستم شما برای دستیابی با سرعت بالا و موضوعات فنی و غیرفنی دیگر مباحثی را ارائه می کند. رجوع به این سایت را قویاً برای افرادی که از طریق خانگی به اینترنت متصل می شوند، توصیه می کنیم.

■ درباره امنیت شبکه خانگی

www.cert.org/tech_tips/home_networks.html

این سایت متعلق به تیم واکنش سریع (اضطراری) کامپیوتری در دانشگاه کارنگی ملون است. این سایت یکی از جامع ترین راهنماها برای حفاظت از کامپیوتر خانگی شما ارائه میکند.

■ درباره امنیت مکینتاش

www.securemac.com

این سایت شامل حجم بالایی از نکات ایمنی و ابزارهای امنیتی برای کامپیوترهای مکینتاش است.

■ درباره امنیت مایکروسافت

www.microsoft.com/security/

این سایت شامل آخرین مشاوره ها و ابزارهای امنیتی برای ویندوز و دیگر محصولات مایکروسافت است.

■ منابع این راهنما

symantecAntivirus:
www.symantec.com
McAffeeAntivirus:www.mcaffee.com
Ad-ware:http://
www.lavas0ftusa.com
Zone Alarm:http://
www.zonelabs.com/
Black Ice:http//
www.blackice.lss.net/

در زیر روش های حفاظتی برای کامپیوتر شما ارائه می شود.

■■■

سطوح حفاظت کامپیوتر

روزآمد کردن سیستم عامل
نرم افزار ضد ویروس
دیواره آتش

↓

اینترنت

↓

الزامات ← روزآمد کردن ضد ویروس و نرم افزار سیستم عامل
پیشتیبانی از داده
ذخیره داده حساس به صورت آف لاین
پست الکترونیک مشکوک را باز نکنید

هشدار ← از گذر واژه خوب استفاده کنید