چند عادت خوب امنیتی

انسان عصر اطلاعات می بایست در کنار استفاده از فن آوری های متعدد، سعی نماید برخی عادات و حرکات پسندیده را برای خود اصل قرار داده و با تکرار مدوام آنان، امکان و یا بهتر بگوئیم شانس خرابی اطلاعات و یا کامپیوتر را کاهش دهد. دستیابی به یک کامپیوتر به دو صورت فیزیکی و از راه دور، امکان پذیر می باشد. شما می توانید به سادگی افرادی را که قادر به دستیابی فیزیکی به سیستم شما می باشند را شناسایی نمائید. آیا شناسایی افرادی که قادرند از راه دور به سیستم شما متصل گردند، نیز امری ساده است؟ پاسخ سوال فوق، منفی است و شناسائی افرادی که از راه دور به سیستم شما متصل می شوند، به مراتب مشکل تر خواهد بود. اگر شما کامپیوتر خود را به یک شبکه متصل نموده اید، قطعاً در معرض تهدید و آسیب خواهید بود. استفاده کنندگان کامپیوتر و کاربران شبکه های کامپیوتری (خصوصاً اینترنت)، می توانند با رعایت برخی نکات که می بایست به عادت تبدیل شوند، ضریب مقاومت و ایمنی سیستم خود را افزایش دهند. در ادامه به برخی از این موارد اشاره می گردد :

- قفل نمودن کامپیوتر زمانی که از آن دور هستیم: شما با قفل نمودن کامپیوتر خود، عرصه را برای افرادی که با نشستن پشت کامپیوتر شما قصد دستیابی بدون محدودیت به اطلاعات شما را دارند، تنگ خواهید کرد.
- قطع ارتباط با اینترنت زمانی که از آن استفاده نمی گردد: پیاده سازی فناوری هائی نظیر اینترنت پرسرعت و مودم‌های کابلی این امکان را برای کاربران فراهم نموده است که همواره به اینترنت متصل و اصطلاحاً online باشند. این مزیت دارای چالش‌های امنیتی خاص خود نیز می باشد. باتوجه به این که شما بطور دائم به شبکه متصل می باشید، مهاجمان و ویروس‌ها فرصت بیشتری برای یافتن قربانیان خود خواهند داشت. در صورتی که کامپیوتر شما همواره به اینترنت متصل است. می بایست در زمانی که قصد استفاده از اینترنت را ندارید، اتصال خود را غیر فعال نمایید. فرآیند غیرفعال نمودن اتصال به اینترنت به نوع ارتباط ایجاد شده، بستگی دارد. چنانچه اطلاعات شما اهمیت زیادی دارد از اتصال سیستم به اینترنت اجتناب کنید.
- بررسی تنظیمات امنیتی: اکثر نرم افزارها نظیر برنامه های مرورگر و یا پست الکترونیکی، امکانات متنوعی را به منظور پیکربندی سفارشی متناسب با شرایط و خواسته استفاده کنندگان، ارائه می نمایند. در برخی موارد همزمان با فعال نمودن برخی از گزینه ها از یک طرف امکان استفاده از سیستم راحت تر شده و از طرف دیگر ممکن است احتمال آسیب پذیری شما در مقابل حملات، افزایش یابد. در این رابطه لازم است تنظیمات امنیتی موجود در نرم افزار را بررسی نموده و گزینه هائی را انتخاب نمائید که علاوه بر تأمین نیاز شما، آسیب پذیری سیستم شما در مقابل حملات را

افزایش ندهد. در صورتی که یک Patch و یا نسخه جدیدی از یک نرم افزار را بر روی سیستم خود نصب می نمائید، ممکن است تغییراتی را در تنظیمات انجام شده اعمال نماید، می بایست بررسی مجدد در خصوص تنظیمات امنیتی را انجام داده تا این اطمینان حاصل گردد که سیستم دارای شرایط مناسب و مقاوم در مقابل تهدیدات است.

- از دانلود کردن نرم‌افزارها از سایت‌های ناشناس و نصب آنها بر روی سیستم جداً خودداری نمایید.