



به نظر شما به منظور افزایش ایمن سازی و حفاظت مطلوب اطلاعات موجود بر روی یک کامپیوتر، صرفاً می‌بایست در انتظار معجزه ای بود که از آستین نرم افزار و یا سخت افزار بیرون خواهد آمد؟ ما به عنوان عوامل انسانی و افرادی که مشهور به کاربران کامپیوتر شده ایم، چه نوع تغییری را در رفتار خود می‌بایست انجام داده تا ما هم سهمی در پیشگیری از فجایع اطلاعاتی را داشته باشیم؟ آیا می‌بایست برخی عادات را ترک و برخی دیگر را ملکه ذهن خود نماییم؟ انسان عصر اطلاعات می‌بایست در کنار استفاده از فن آوری‌های متعدد، سعی نماید که برخی عادات و حرکات پسندیده را برای خود اصل قرار داده و با تکرار مداوم 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 می‌باشد. شما می‌توانید بسادگی افرادی را که قادر به دستیابی فیزیکی به سیستم و کامپیوتر شما می‌باشند را شناسائی نمائید. (مثلاً افراد خانواده و یا همکاران) آیا شناسائی افرادی که می‌توانند از راه دور به سیستم شما متصل گردند، نیز امری ساده است؟ پاسخ سوال، منفی است و شناسائی افرادی که از راه دور به سیستم شما متصل می‌شوند، بمراتب مشکل تر خواهد بود. اگر شما دارای یک کامپیوتر هستید و آن را به یک شبکه (مثلاً اینترنت) متصل نموده اید، قطعاً در معرض تهدید و آسیب خواهید بود. استفاده کنندگان کامپیوتر و کاربران شبکه های کامپیوتری (خصوصاً اینترنت)، می‌توانند با رعایت برخی نکات که می‌بایست به عادت تبدیل شوند، ضریب مقاومت و ایمنی سیستم خود را افزایش دهند. در ادامه به برخی از این موارد اشاره می‌گردد.

قفل نمودن کامپیوتر زمانی که از آن دور هستیم : حتی اگر صرفاً برای چند دقیقه کامپیوتر خود را ترک می‌کنید، زمان کافی برای افراد دیگر به منظور آسیب رساندن به اطلاعات شما وجود خواهد داشت. شما با قفل نمودن کامپیوتر خود، عرصه را برای افرادی که با نشستن پشت کامپیوتر شما قصد دستیابی بدون محدودیت به تمامی اطلاعات شما را دارند، تنگ خواهید کرد.

قطع ارتباط با اینترنت زمانی که از آن استفاده نمی‌گردد : پیاده سازی فناوری هائی نظیر DSL و مودم های کابلی این امکان را برای کاربران فراهم نموده است که همواره به اینترنت متصل و اصطلاحاً online باشند. این مزیت دارای چالش های امنیتی خاص خود نیز می‌باشد. باتوجه به این که شما بطور دائم به شبکه متصل می‌باشید، مهاجمان و ویروس های کامپیوترهای فرصت بیشتری برای یافتن قربانیان خود خواهند داشت. در صورتی که کامپیوتر شما همواره به اینترنت متصل است. می‌بایست در زمانی که قصد استفاده از اینترنت را ندارید، اتصال خود را غیر فعال نمائید. فرآیند غیرفعال نمودن اتصال به اینترنت به نوع ارتباط ایجاد شده، بستگی دارد. مثلاً قطع خط تلفن ارتباطی، خاموش نمودن کامپیوتر یا مودم و ...



بررسی تنظیمات امنیتی: اکثر نرم افزارها نظیر برنامه های مرورگر و یا پست الکترونیکی، امکانات متنوعی را به منظور بیکربندی 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 تامین 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 که ممکن است تغییراتی را در تنظیمات انجام شده، اعمال نماید، می بایست بررسی مجدد در خصوص تنظیمات امنیتی را انجام تا این اطمینان حاصل گردد که سیستم دارای شرایط مناسب و مقاوم در مقابل تهدیدات است.

به منظور افزایش مقاومت سیستم در مقابل خرابی و از دست دادن اطلاعات، می بایست به ابعاد دیگری نیز توجه داشت. برخی مواقع تهدید اطلاعات و در معرض آسیب قرار گرفتن آنان از جانب افراد نبوده و این موضوع به عوامل طبیعی و فنی دیگری بستگی دارد. با اینکه روشی برای کنترل و یا پیشگیری قطعی این نوع از حوادث وجود ندارد ولی می توان با رعایت برخی نکات میزان خرابی را کاهش داد.

حفاظت کامپیوتر در مقابل نوسانات جریان برق: در صورت وجود نوسانات شدید برق، می بایست کامپیوتر را خاموش و کابل های آن را از پریز مربوطه جدا نمود. با اینکه برخی از منابع تغذیه، امکان حفاظت سیستم در مقابل نوسانات برق را افزایش می دهند، ولی آنان به تنهایی به منظور حفاظت سیستم در مقابل نوسانات جریان برق کافی نبوده و می توان در این رابطه از محصولاتی دیگر نظیر ups در زمان ایجاد نوسانات برق و یا قطع برق، استفاده نمود.

backup گرفتن از داده ها: صرف نظر از این که شما خود را در مقابل مسائل ایمنی محافظت نموده باشید، همواره احتمال بروز حوادثی وجود خواهد داشت که باعث از دست دادن اطلاعات می گردد. شما ممکن است حداقل دارای یک مورد تجربه باشید که در آن یک و یا چندین فایل خود را در اثر بروز حادثه ای از دست داده باشید (مثلاً" توسط عملکرد یک کرم و یا ویروس، یک حادثه طبیعی و یا یک مشکل خاص که در سخت افزار سیستم ایجاد شده باشد) تهیه منظم فایل backup بر روی یک CD و یا شبکه، نگرانی های احتمالی را کاهش خواهد داد. تشخیص این که در چه مقاطع زمانی و به چه صورت از اطلاعات backup گرفته شود یک تصمیم شخصی است. در صورتی که شما بطور دائم در حال افزودن و یا تغییر داده های موجود بر روی کامپیوتر می باشید، می توان عملیات backup را با فرکانس بیشتر و در محدوده زمانی کوتاهتری، تکرار نمود.