

## توصیه های حفاظتی و امنیت IT

۱- هرگز از رایانه خود به ویژه در محل کار، بدون رمز عبور (پسورد) استفاده نکنید.

همیشه برای رایانه خود رمز عبور تعیین کرده و آن را طوری تنظیم نمائید که در صورت عدم استفاده از آن به مدت (حداکثر) پنج دقیقه از شما اسم عبور درخواست نماید. این کار مانعی برای دسترسی دیگران به رایانه شما خواهد بود و تا حدودی امنیت سیستم شما را افزایش می دهد.

۲- هرگز از رمز عبور ساده و مشخص استفاده نکنید.

سعی کنید رمز عبورهای سیستم خود را پیچیده و غیرقابل پیش بینی انتخاب کنید. انتخاب رمز عبور با کارکترهای زیاد، با حروف و اعداد، حروف کوچک و بزرگ و با انتخاب آن به زبان دیگر، می تواند امنیت سیستم شما را افزایش دهد.

۳- هرگز اطلاعات محرمانه خود را در فایل های آشکار و سهل الوصول قرار ندهید.

فایل های محرمانه خود را می توانید به صورت پنهان و در زیر مجموعه فایل های سیستمی یا زیر مجموعه سایر برنامه های نصبی سیستم قرار دهید تا به راحتی در اختیار افراد بیگانه قرار نگیرد. در غیر این صورت، احتمال دسترسی راحت به این گونه فایل های همواره متصور است.

۴- هرگز از کامپیوتری که دارای اطلاعات محرمانه و با اطلاعات خصوصی است، برای متصل شدن به اینترنت استفاده نکنید.

همیشه در هنگام متصل شدن به اینترنت خطر سرقت اطلاعات، تخریب اطلاعات به صورت جدی وجود داشته و در صورت بی تفاوتی به این مطلب خطرات جبران ناپذیری سیستم و اطلاعات شما را تهدید می کند.

۵- هرگز کامپیوتر خود را که حاوی اطلاعات محرمانه یا خصوصی است، جهت تعمیر به افراد متفرقه و ناشناس ندهید.

حتماً نسبت به تعمیرکار کامپیوتر خود اطمینان حاصل نموده و سعی کنید شخصاً هنگام تعمیر حضور داشته باشید.

۶- هرگز قطعات آسیب دیده سیستم کامپیوتر خود را (مانند: هارد، فلاپی، سی دی و ...) دور نیاندازید.

حتماً این گونه لوازم از کار افتاده را منهدم کرده و امکان بهره برداری مجدد را از آن ها بگیرید. اغلب کامپیوترهای مستعمل و از رده خارج شده دارای اطلاعات ارزشمندی است که در هنگام تعویض یا فروش بر اثر سهل انگاری در سیستم ها باقی مانده است. همچنین امکان بازیافت اطلاعات از حافظه های پاک شده سیستم وجود داشته و صرف پاک کردن یا فرمت کردن سیستم نمی توان از پاک شدن صد در صد آن ها اطمینان داشت. بنابراین بعضی از افراد تصور می کنند با پاک کردن هاردهای مستعمل تمام اطلاعات آن ها از بین رفته و می توانند آن ها را دور ریخته یا به فروش برسانند.

۷- هرگز به تماس های تلفنی از طریق اینترنت اعتماد نداشته باشید.

امروز اغلب تلفن های خارج از کشور توسط تماس های تلفنی اینترنتی صورت می گیرد که کارتهای خدماتی آن ها در همه جا قابل دسترس می باشد. از آن جا که شرکت های خدمات اینترنت (آی-اس-پی) و کشورهای سرویس دهنده (بک بن) توانایی استراق سمع

۸- هرگز از کامپیوتر مخصوص اینترنت برای کارهای متفرقه استفاده ننمائید. در نظر داشته باشید که مودم، پرینتر، اسکنر و بعضی از اجزای داخلی کامپیوتر «آی-پی» پذیر بوده و می تواند اطلاعات خود را به آدرس برنامه ریزی شده از طریق اینترنت ارسال کنند. بنابراین ممکن است

نامه‌ای که تایپ کرده و پرینت گرفته‌اید و حتی از کامپیوتر خود را که پاک کرده‌اید، بعد از آن که به اینترنت متصل می‌شوید، به آدرس برنامه ریزی شده ارسال گشته بدون آن که شما از آن مطلع گردید.

۹- هرگز نسبت به محافظت و نگهداری نسخه ذخیره اطلاعات (backup) بی تفاوت نباشید.

معمولاً به خاطر محافظت از اطلاعات و پیش‌گیری از تخریب آن‌ها اقدام به تهیه نسخه‌های ذخیره می‌نمایند. حفاظت و نگهداری این نسخه‌ها حتی از اطلاعاتی که در سیستم‌ها نگهداری می‌شوند با اهمیت‌تر می‌باشد. زیرا این اطلاعات به صورت آماده و بدون دردسر می‌باشند. سهل انگاری در نگهداری از این نسخه‌های ذخیره بعضاً معضلات جبران ناپذیری در بر خواهد داشت.

۱۰- هرگز در مواقع غیرضروری سیستم خود را به شبکه اینترنت متصل ننمائید.

اغلب در ارتباطات لیزلاین و شبکه‌ای، ارتباط اینترنتی به صورت پیوسته و شبانه روزی است. اما با توجه به تهدیداتی که از این طریق برای سیستم شما متصور است، در مواقعی که نیازی به ارتباط با اینترنت ندارید، آن را قطع نمائید تا از گزند هکرها و جاسوسان اینترنتی و عوامل بیگانه در امان باشید. هکرها توانائی فعال‌سازی میکروفن و دوربین (وب کم) شما را بدون توافق با شما را دارند. لذا با توجه به متصل بودن بی‌مورد و طولانی مدت سیستم شما به اینترنت این‌گونه خطرات همواره متصور است.

۱۱- هرگز نسبت به تهیه نسخه ذخیره از اطلاعات درون رایانه خود مسامحه نکنید.

رایانه‌ها ابزار قابل اطمینانی نیستند و همواره احتمال صدمه دیدن آن‌ها متصور است لذا همیشه سعی کنید از اطلاعات داخل سیستم خود یک نسخه ذخیره داشته باشید تا در صورت بروز هرگونه اختلالی اطلاعات شما در اختیارتان باشد.

۱۲- هرگز به موارد شناخته نشده در اینترنت پاسخ ندهید.

ایمیل‌های ناشناخته یکی از موارد بوده که هرگز نباید آن‌ها را گشود، زیرا در مواردی با گشودن ایمیل یا یک تصویر اینترنتی تروجانی از این طریق وارد سیستم شما گشته و مراحل کار جاسوسی و نفوذ به سیستم شما را آغاز می‌نماید یا پنجره‌هایی که در خلال کار با اینترنت به صورت ناخواسته ظاهر گشته یا درخواست‌های اشتراک در سایت، شما را ترغیب به دادن نام کاربر و نام عبور می‌نماید که از این طریق اطلاعات مربوط به رمز عبور شما را در اختیار گرفته و از آن بهره برداری کنند.