توصیه حفاظتی در امنیت رایانه

1. 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 می‌دهد.
2. 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 یا انتخاب آن به زبان دیگر، می‌تواند امنیت سیستم شما را افزایش دهد.
3. هرگز اطلاعات محرمانه خود را در فایل‌های آشکار و سهل الوصول قرار ندهید.
فایل‌های محرمانه خود را می‌توانید به‌صورت پنهان و در زیر مجموعه فایل‌های سیستمی یا زیر مجموعه سایر برنامه‌های نصبی سیستم قرار دهید تا به‌راحتی در اختیار افراد بیگانه قرار نگیرد. در غیر این صورت، احتمال دسترسی راحت به این‌گونه فایل‌های همواره متصور است.
4. 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 به‌صورت جدی وجود داشته و در صورت بی تفاوتی به این مطلب خطرات جبران ناپذیری سیستم و اطلاعات شما را تهدید می‌کند.
5. 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.
6. هرگز قطعات آسیب دیده سیستم کامپیوتر خود را (مانند: هارد، فلاپی، سی دی و ...) دور نیاندازید.
حتما این‌گونه لوازم از کار افتاده را منهدم کرده و امکان بهره برداری مجدد را از آن‌ها بگیرید. اغلب کامپیوترهای مستعمل و از رده خارج شده دارای اطلاعات ارزشمندی است که در هنگام تعویض یا فروش بر اثر سهل انگاری در سیستم‌ها باقی مانده است. هم‌چنین امکان بازیافت اطلاعات از حافظه‌های پاک شده سیستم وجود داشته و صرف پاک کردن یا فرمت کردن سیستم نمی‌توان از پاک شدن صد در صد آن‌ها اطمینان داشت. بنابراین بعضی از افراد تصور می‌کنند با پاک کردن هاردهای مستعمل تمام اطلاعات آن‌ها از بین رفته و می‌توانند آن‌ها را دور ریخته یا به فروش برسانند.
7. هرگز به تماس‌های تلفنی از طریق اینترنت اعتماد نداشته باشید.
امروز اغلب تلفن‌های خارج از کشور توسط تماس‌های تلفنی اینترنتی صورت می‌گیرد که کارت‌های خدماتی آن‌ها در همه جا قابل دسترس می‌باشد. از آن‌جا که شرکت‌های خدمات اینترنت (آی- اس- پی) و کشورهای سرویس دهنده (بک بن) توانایی استراق سمع تمامی مکالمات تلفنی را دارند. استفاده از این

ارتباطات نیز ناامن و غیرمطمئن می‌باشد.

8. هرگز از مشخصات اصلی خود در محیط اینترنت استفاده نکنید.

در هنگام حضور افراد در خارج از کشور یکی از راه‌های به‌دست آوردن اطلاعات از آن‌ها، مراجعه به فضای اینترنت می‌باشد. در صورتی که مشخصات شما در یک سایت یا ایمیل یا .... مشاهده گردد. اطلاعات با ارزشی نسبت به شما می‌تواند به‌دست آید.

9. هرگز از کامپیوتر مخصوص اینترنت برای کارهای متفرقه استفاده ننمائید.

در نظر دشته باشید که مودم، پرینتر، اسکنر و بعضی از اجزای داخلی کامپیوتر «آی- پی» پذیر بوده و می‌تواند 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 آن‌که به اینترنت متصل می‌شوید، به آدرس برنامه ریزی شده ارسال گشته بدون آن‌که شما از آن مطلع گردید.

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

معمولاً به‌خاطر 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 به‌صورت آماده و بدون دردسر می‌باشند. سهل انگاری در نگهداری از این نسخه‌های ذخیره بعضاً معضلات جبران ناپذیری در بر خواهد داشت.

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

اغلب در ارتباطات لیزلاین و شبکه‌ای، ارتباط اینترنتی به‌صورت 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.

12. 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.

13. 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 به‌صورت 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.

منبع : http://ui.ac.ir/herasat