امنیت اطلاعات

امروزه امنیت اطلاعات در سیستم های کامپیوتری به عنوان یکی از مسائل مهم مطرح است و می بایست به مقوله امنیت اطلاعات نه به عنوان یک محصول بلکه به عنوان یک فرآیند نگاه گردد. بدون شک اطلاع رسانی در رابطه با تهدیدات، حملات و نحوه برخورد با آنان، دارای جایگاهی خاص در فرآیند ایمن سازی اطلاعات بوده و لازم است همواره نسبت به آخرین اطلاعات موجود در این زمینه خود را به روز نمائیم.

هر روزه اخبار جدیدی در مورد حملات و تهدیدات رایانه ای در رسانه های مختلف انتشار می یابد. این تهدیدات شامل ویروس های جدید و یا انواع هک و نفوذ در سیستم های کامپیوتری، کلاهبرداری ها، سرقت ها، جعل ها و نظایر آنهاست. انتشار این گونه اخبار باعث شیوع اضطراب و نگرانی در بین کاربرانی می شود که به صورت مستمر از کامپیوتر بهره می گیرند و یا اطلاعاتی ارزشمند (شخصی یا سازمانی) بر روی رایانه های خود دارند.

فناوری اطلاعات در کنار تسهیلات و امکانات فوق العاده ای که فراهم آورده است، می تواند در صورت عدم توجه و رعایت برخی نکات، مضرات و گاه خسارات جبران ناپذیری نیز به بار آورد. لذا کاربران کامپیوتر و کاربران شبکه های کامپیوتری (خصوصاً اینترنت)، می بایست در کنار استفاده از فن آوری های متعدد، سعی نمایند 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 داده و مانع نفوذ و یا سو استفاده شوند. بی توجهی به امنیت اطلاعات می تواند عواقب زیر را به دنبال داشته باشد:

- **نفوذ به شبکه و دسترسی به اطلاعات طبقه بندی شده**
- **تخریب و دستکاری اطلاعات موجود در سیستم و نرم افزارها**
- **اشغال پهنای باند و اتلاف پهنای باند**
- **سوء استفاده های آموزشی، مالی، اداری و... از طریق نفوذ به سیستم های مربوطه**

با توجه به اهمیت اطلاع رسانی و آگاهی رسانی و به منظور رعایت نکات امنیتی هنگام کار با کامپیوتر و شبکه اینترنت و جهت پیشگیری از وقوع حوادث و ایراد خسارت های احتمالی، توصیه نامه هایی توسط مرکز مدیریت آمار و فن آوری اطلاعات دانشگاه تهیه شده که به طور مستمر در اختیار کاربران دانشگاه قرار خواهد گرفت.

انتظار می رود با توجه به اهمیت موضوع کلیه کاربران کامپیوتر و اینترنت دانشگاه به طور جدی نسبت به مطالعه و رعایت نکات مندرج در این توصیه نامه ها اقدام نمایند.

ضمناً پرسنل دانشگاه می توانند جهت به اشتراک گذاردن مطالب مفید خود در زمینه نکات امنیتی، مطالب خود را به آدرس پست الکترونیکی itsm@kaums.ac.ir ارسال نموده تا در دسترس سایر پرسنل نیز قرار گیرد.

بدیهی است مسئولیت عدم رعایت موارد توصیه شده بر عهده کاربر می باشد.

در مقوله امنیت جمله‌ای است که می‌گوید: «اگر هکر (یا افراد مغرض و سودجو) بتواند کنترل فیزیکی کامپیوتر را به دست گیرد، بازی تمام است». وقتی که دستگاه به دست این افراد افتاد، آنها می‌توانند با استفاده از ابزاری که در دست دارند به اطلاعات سیستم شما دسترسی پیدا کنند. از این رو، پیش از اینکه به دیگر روش‌های امنیت فکر کنید، باید امنیت فیزیکی مساله اصلی تان باشد.

از این رو:

- پس از اتمام کار با رایانه حتما نام کاربری خود را logoff نمایید.
- در مواقعی که به مدت طولانی از رایانه استفاده نمی کنید حتما آن را خاموش کنید.
- در صورتی که از اتاق خارج می شوید در صورت امکان درب آن را نیز ببندید.
- هنگامی که قصد ترک موقتی رایانه خود را (حتی برای چند لحظه) دارید، ویندوز خود را lock نمایید. (با استفاده از کلید های ترکیبی Windows Key +L)
- در صورتیکه چند نفر از یک رایانه استفاده می کنید، هر یک با نام کاربری خود login شوید.
- از گذاشتن مشخصات فردی، عکس، شماره تلفن، ایمیل شخصی و ... بر روی سیستم تان خودداری کنید.
- به هیچ عنوان اطلاعات طبقه بندی شده، عکس ها و فیلم های خانوادگی خود را در رایانه اداری نگهداری نکنید.
- تحت هیچ شرایطی رمز عبور مربوط به کامپیوتر، ایمیل، اینترنت و مجموعه نرم افزارهای اداری خود را حتی در اختیار همکاران خود قرار ندهید. به اشتراک گذاردن رمز عبور می تواند عواقب جبران ناپذیری برای شما داشته باشد.
- حتماً جهت ورود به کامپیوتر اداری خود رمز عبوری را انتخاب نمایید تا دسترسی افراد به اطلاعات موجود در کامپیوترتان امکانپذیر نباشد. دسترسی هر فرد به کامپیوترتان حتی برای چند دقیقه می تواند عواقب زیادی برای شما ایجاد کند.
- به هیچ عنوان و تحت هیچ شرایطی کامپیوتر اداری خود را (حتی برای چند دقیقه) در اختیار سایر افراد قرار ندهید. کافی است در همین فاصله خیلی کم، اطلاعاتی از دستگاه شما به سرقت رفته و یا اطلاعات خارج از چهارچوب اداری بر روی سیستم شما کپی گردد. مسئولیت اطلاعات موجود بر روی سیستم شما بر عهده خود شماست.
- اجازه ندهید هر کسی کول دیسک یا فلش مموری خود را به رایانه شما وصل کند. بسیاری از کرم ها یا نرم افزارهای جاسوسی به محض اتصال کول دیسک به رایانه، کار خود را شروع می کنند.
- در صورت سرقت قطعات کامپیوتری یا مفقود شدن، حتما مراتب را به مسئول واحد خود اطلاع دهید.
- در صورت نیاز به تعمیرات قطعات کامپیوتری در خارج از دانشگاه حتما با کارشناس IT واحد خود هماهنگی لازم را انجام دهید.

آیا می دانید:

- *آیا می دانید:* ارسال، انتشار، ذخیره سازی و یا نگهداری فایل ها، عکس ها و فیلم های دارای محتوای مغایر با اصول قانون اساسی و نظام جمهوری اسلامی ایران از مصادیق جرائم رایانه ای محسوب می شود؟
- *آیا می دانید:* نصب و انتشار فیلترشکن ها و آموزش روش های عبور از سامانه های فیلترینگ، محتوای مجرمانه و نشانی های اینترنتی مسدود شده از مصادیق جرائم رایانه ای محسوب می شود؟
- *آیا می دانید:* اطلاعات بر روی رایانه شما حتی بعد از حذف نیز قابل بازیابی خواهند بود.
- *آیا می دانید:* بر روی بستر اینترنت میلیون ها نفر قادرند به اطلاعات رایانه شما دسترسی داشته باشند.
- *آیا می دانید:* هکر ها به راحتی می توانند از ارتباط به ظاهر ساده اینترنتی به سیستم شما نفوذ کنند. بنابراین در صورتی که نیاز به اینترنت ندارید، حتما ارتباط اینترنت خود را قطع نمایید.
- *آیا می دانید:* در تمام مدتی که رایانه از طریق نام کاربری شما به اینترنت متصل است، استفاده هر شخص دیگری از آن رایانه و همچنین محل های بازدید شده و امور انجام شده به نام شما ثبت می گردد.
- *آیا می دانید:* به راحتی و از طریق Email های ارسالی می توانند به اطلاعات رایانه های شما دسترسی پیدا نمایند.
- *آیا می دانید:* یک نرم افزار یا فایل می تواند یک جاسوس یا عامل مخرب باشد، پس بدون هماهنگی با مسئولین و کارشناس مربوطه هیچ نرم افزار یا فایلی را بر روی رایانه خود ذخیره ننمایید.
- *آیا می دانید:* عدم استفاده از یک رمز عبور مناسب می تواند چه عواقبی برای شما ایجاد کند. کافی است نفوذگر با حدس زدن، به رمز عبور شما دسترسی پیدا کند.
- *آیا می دانید:* قانون جرائم رایانه ای در تاریخ ۱۳۸۸/۱۱/۱۱ در ۳ بخش و ۵۶ ماده به تصویب رسیده است.