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 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 داده و مانع نفوذ و یا سو استفاده را بگیرند. چرا که بی توجهی به امنیت اطلاعات می تواند موارد 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**

به منظور اطلاع رسانی و جهت پیشگیری از وقوع حوادث و ایراد خسارت های احتمالی، مطالعه و رعایت نکات ذیل توصیه می گردد.

امنیت فیزیکی

در مقوله امنیت جمله‌ای است که می‌گوید: «اگر هکر (یا افراد مغرض و سودجو) بتوانند 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 هارد دیسک و هر اطلاعاتی که به کامپیوتر آمده و از آن خارج می‌شود دسترسی یابند. از این رو، پیش از اینکه به دیگر روش‌های امنیت فکر کنید، امنیت فیزیکی بایستی 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.
- اجازه ندهید اشخاص دیگر پشت میز شما نشسته و از رایانه استفاده کنند.
- در صورتیکه چند نفر از یک رایانه استفاده می کنند، هر یک با نام کاربری خود login نمایند.

- اجازه ندهید هر کس 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.
- با توجه به اینکه لپ تاپ ها از آسیب پذیری و احتمال سرقت بیشتری برخوردارند، رعایت نکات فوق اهمیت بیشتری دارد.
- در صورت سرقت قطعات کامپیوتری یا مفقود شدن، حتما مرکز فناوری اطلاعات دانشگاه را مطلع سازید.

هارد دیسک

- در زمان کار کردن با رایانه آنرا تکان ندهید و یا به کیس ضربه نزنید چون باعث ایجاد بد سکتور و کرش کردن هارد می شود.
- از بازکردن درب کیس در هر شرایطی خودداری نموده و در صورت نیاز به کارشناسان IT مراجعه نمایید.
- جهت جلوگیری از خسارات ناشی از نوسانات برق، حتما از محافظ برق ا ستفاده نمایید.
- از گذاشتن مشخصات فردی، عکس، شماره تلفن، ایمیل شخصی و ... تا حد امکان خودداری کنید.
- اطلاعات طبقه بندی شده و فیلمهای خانوادگی را در رایانه نگهداری نکنید.
- فایلهای مهم نباید در درایو روت و یا درایوی که ویندوز در آن نصب است (مثلا C) قرار گیرند .
- Desktop یا My Document محل مناسبی برای نگهداری فایل ها نیستند. اسناد خود را در این مکان ها نگهداری نکنید.
- هر چند وقت یکبار هارد را Defrag کنید تا هم سرعت سیستم بیشتر شود و هم کارآیی هارد بالاتر رود .
- در صورت نیز به تعمیرات قطعات کامپیوتری در خارج از دانشگاه حتما با مرکز فناوری اطلاعات دانشگاه هماهنگی لازم را انجام دهید.

کول دیسک ها و فلش مموری

به خاطر داشته باشید که کول دیسک، فلش مموری و نظایر آن تنها ابزارهای انتقال اطلاعات هستند نه ابزار نگهداری اطلاعات. پس هیچ گاه اطلاعات مهم خود را در فلش مموری نگه ندارید چرا که در موارد زیادی ، ویروس ها تمامی محتوای فلش را ناپدید می کنند ، فرمت آنها را تغییر می دهند که عموما باعث خرابی فایل می شود و یا شرایطی را اعمال می کنند که مجبور به فرمت کردن فلش مموری می شوید ، بدیهیست در این زمان اطلاعات شما نیز از دست می رود پس همیشه اطلاعات مهم خود را در کامپیوتر شخصی نگه داشته و از آن نسخه پشتیبان نیز تهیه کنید.

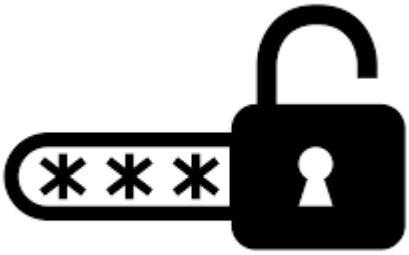
- یکی از بهترین ابزارهای انتقال ویروس به رایانه ها، کول دیسک ها هستند. مثلا اکثر ویروسها مخصوصا Autorun فقط با اتصال کول دیسک به رایانه ، به راحتی آنرا ویروسی می کنند. همیشه قبل از استفاده از آن حتما آن را ویروس یابی نموده و برای بازنمودن آن به جای دوبار کلیک از نوار آدرس آن را باز کنید.

- فلشها بدلیل حجم بسیار بالا و قابلیت اتصال سریع به رایانه و اندازه کوچکشان همیشه یک ریسک امنیتی برای اطلاعات سیستم به حساب می آیند، چرا که سرقت یک کول دیسک به مراتب راحت تر و سریعتر از سایر رسانه های ذخیره ساز است و عبور آن از فیلترهای امنیتی نیز آسان می باشد.
- در صورت امکان از کول دیسکهای با قابلیت رمز گذاری استفاده شود.
- فلش خود را در اختیار دیگری قرار ندهید .
- یک فایل حاوی نام و نشانی خود در فلش قرار دهید تا اگر گم شد قابل شناسایی باشد.

امنیت ایمیل

- این قانون ساده را پیروی کنید، «اگر فرستنده نامه را نمی شناسید، نسبت به نامه و پیوست های آن بسیار با دقت عمل نمایید».
- برای امنیت بیشتر حتی اگر فرستنده نامه آشنا باشد هم باید با احتیاط بود. اگر عنوان نامه نا آشنا و عجیب باشد، و بالاخص در صورتی که نامه حاوی لینک های غیرمعمول باشد باید با دقت عمل کرد. لذا جهت پیشگیری از ورود ویروس ها و کدهای مخرب احتمالی از بروز بودن آنتی ویروس سیستم مطمئن شوید و به هنگام اعلام پیغام توسط آنتی ویروس در صورت لزوم گزینه مورد نظر را جهت از بین بردن اثر مخرب ایمیل انتخاب نمایید.
- اکثر اوقات ضمیمه نامه های ارسالی از طرف افراد ناشناس حاوی کدهای مخرب است که ممکن است در صورت اجرا فایل های موجود در رایانه شما را از بین برده و یا اطلاعات شما را به سرقت ببرد. لذا از دانلود کردن (بازکردن) نامه هایی که از طرف افراد ناشناس برای شما ارسال می گردد خودداری نمایید.
- در صورتیکه همراه ایمیل فایلی ضمیمه شده است، قبل از باز نمودن آن از هر نوعی که باشد، حتما آن را دانلود کرده و از طریق آنتی ویروس از آلوده نبودن فایلها به ویروس مطمئن شوید. چرا که بسیاری از ویروسها در داخل فایلهای پیوست پست الکترونیکی پنهان می شوند.
- به درخواست های غیرمنطقی مذکور در ایمیل ها هرگز پاسخ ندهید. ممکن است ایمیلی جعلی در یافت کنید که خود را نماینده یکی از سایت های معتبر یا دانشگاه علوم پزشکی معرفی کرده و از شما نام کاربری و رمز عبورتان را بخواهد و یا شما را برنده جایزه ای اعلام نموده و از شما درخواست اعلام مشخصات و یا واریز وجه نماید. دانشگاه و زیرمجموعه های وابسته به آن به هیچ عنوان به کاربران خود به صورت موردی و تک تک ایمیلی ارسال نمی کنند. (مگر ایمیل های عمومی مانند اطلاع رسانی ها و نظایر آن) لذا هر گونه ایمیلی که با اسم یا عنوان دانشگاه یا مجموعه های وابسته به آن دریافت کردید که از شما در خواست پسوورد دارد پاسخ نداده و مرکز فناوری اطلاعات را در جراین قرار دهید.
- پس از اتمام کار با نرم افزار با کلیک نمودن بر روی گزینه logout به طور صحیح از ایمیل خود خارج شوید تا از سوء استفاده های احتمالی پیشگیری شود.

استفاده از رمز عبور مناسب



- رمز عبور تنها در صورتی دسترسی غریبه ها به منابع موجود را محدود می کند که حدس زدن آن به سادگی امکان پذیر نباشد. برخی افراد با توجیه فراموشی و کم حافظگی رمز عبور در اختیار خود را بسیار ساده (مثلا ۱۲۳ یا ۱۲۳۴۵ یا مشابه آن) انتخاب می کنند. در حالیکه اگر فرد از خطرات و یا سو استفاده های احتمالی ناشی از آن آگاه باشد هرگز چنین رمزعبوری را انتخاب نمی نماید. پس رمز عبور خود را به نحوی انتخاب کنید که موارد زیر رعایت شده باشد:
- رمز عبور باید حداقل شامل ۸ حرف بوده و مخلوطی از حروف کوچک، بزرگ، اعداد و کاراکترهای ویژه باشد. (مانند xk27D8Fy)
- از رمزهای عبوری که مبتنی بر اطلاعات شخصی هستند استفاده نکنید. این نوع رمزهای عبور به سادگی حدس و تشخیص داده می شوند.
- رمز عبورهای پیش فرض را حتما تغییر دهید.
- رمز عبورهای خود را به صورت دوره ای (مثلا ماهانه یا ۲ ماه یکبار) عوض نمایید.
- رمز عبورهای خود (مثلا رمز عبور اینترنت، ایمیل، ویندوز، اتوماسیون اداری و سایر نرم افزارهای دیگر) را تحت هیچ شرایطی در اختیار دیگران قرار ندهید. عواقب سوء استفاده از نام کاربری و رمز عبور شما توسط سایر کاربران بر عهده خودتان می باشد.
- از یک رمز عبور در بیشتر از یک جا استفاده نکنید. در این صورت اگر یکی از گذرواژه های شما لو برود، همه منابع در اختیار شما در معرض خطر قرار نخواهند گرفت.
- در حفظ و نگهداری و مخفی نگهداشتن رمز عبور خود دقت نموده و از نوشتن رمز عبور بر روی کاغذ و گذاشتن آن بر روی میز محل کار، نزدیک کامپیوتر و یا چسباندن آن بر روی کامپیوتر، جداً اجتناب کنید.
- ترجیحاً از یادداشت نمودن آن خودداری نموده و از ذخیره کردن (save) آن در محیط مرورگر اینترنتی خودداری نمائید.
- هنگام استفاده از نرم افزارها یا وبسایت هایی که از شما رمز عبور می خواهند، بعد از واردنمودن آن تیک ذخیره را هرگز فعال نکنید.
- محافظت از کامپیوتر در برابر نفوذ با استفاده از حفاظ(Firewall)
- فایروال به عنوان حفاظ و دیواری مجازی بین رایانه و دنیای بیرون ایجاد می کند. این حفاظ، داده های غیر مجاز و یا داده هایی که به صورت بالقوه خطرناک می باشند را فیلتر کرده و سایر اطلاعات را عبور می دهد. علاوه بر این حفاظ در شرایطی که کامپیوتر به اینترنت وصل است، مانع دسترسی افراد غیرمجاز به کامپیوتر می شود. پس دیوار آتش یا firewall ویندوز را تحت هیچ شرایطی غیر فعال نکنید.

- پیکربندی فایروال خود را به دقت انجام دهید تا از نفوذ به رایانه شما جلوگیری شود.
- رعایت حقوق دسترسی در به اشتراک گذاری (Share) منابع رایانه
- سیستم های عامل این امکان را برای کاربران خود فراهم می آورند که با هدف به اشتراک گذاری فایل، دسترسی دیگران را از طریق شبکه و یا اینترنت به دیسک سخت محلی فراهم آورند. این قابلیت امکان انتقال ویروس از طریق شبکه را فراهم می آورد. از سوی دیگر در صورتی که کاربر دقت کافی را در به اشتراک گذاشتن فایل ها به عمل نیاورد، امکان مشاهده فایل های خود را به دیگرانی که مجاز نیستند ایجاد می کند. بنابراین فقط از پوشه IT_Share موجود در رایانه خود به منظور به اشتراک گذاری فایل ها استفاده نمایید.
- جهت انتقال اطلاعات محرمانه (مانند سوالات امتحانی اساتید و ...) در شبکه هرگز از IT_Share استفاده نکنید.
- محتویات غیرضروری پوشه IT_Share را حتما پاک کنید.
- به اشتراک گذاری پرینتر به نحوی انجام شود که فقط کاربرانی که مجاز به پرینت گرفتن از سیستم شما هستند به آن دسترسی داشته باشند.

قطع اتصال به اینترنت در مواقع عدم استفاده

- قطع اتصال کامپیوتر به اینترنت در شرایطی که نیازی به آن نیست احتمال اینکه کسی به دستگاه شما دسترسی داشته باشد را از بین می برد.
- مهم تر از آن در تمام مدتی که رایانه از طریق نام کاربری شما به اینترنت متصل است، استفاده هر شخص دیگری از آن رایانه و محل های بازدید شده و امور انجام شده به نام شما ثبت می گردد.

تهیه پشتیبان از داده های موجود بر روی کامپیوتر

- از آنجا که هیچ شخصی و هیچ رایانه ای در برابر حملات، سرقت ها یا اشتباهات انسانی و از دست رفتن اطلاعات مصون نیست،از اطلاعات ارزشمند خود نسخه پشتیبان یا بک آپ تهیه کنید.
- برای بایگانی از هارد اکسترنال و یا لوح فشرده (CD یا DVD) استفاده کنید .
- هارد دیسک جانبی را در محلی مناسب قرار دهید.
- در صورتیکه به لوح فشرده حاوی اطلاعات نیاز ندارید ابتدا آن را شکسته و سپس دور بیندازید.
- به خاطر داشته باشید با گذشت زمان لایه های پلاستیکی لوح های فشرده خشک می شود و اطلاعات از بین رفته و قابل بازیافت نمی باشند.
- استفاده زیاد از لوح های فشرده باعث خش افتادن می شود و آن را غیرقابل استفاده می نماید.

آنتی ویروس

- به منظور حفاظت از کامپیوتر و اطلاعات خود در مقابل ویروسها، Worm ها و Trojanهای شناخته شده، نصب آنتی ویروس الزامی است .
- اگر ویروسها و یا Trojan های جدیدی تولید شده باشند که در نرم افزار آنتی ویروس هنوز روشهای شناسایی آنها موجود نباشد ، آن آنتی ویروس از شناسایی آن ناتوان است و باید از آخرین آپدیت آنتی ویروس ها استفاده نمود. لذا پس از نصب آنتی ویروس تنظیمات بروزرسانی آن را چک کرده و از درستی آن مطمئن شوید.
- جهت جلوگیری از ورود ویروس ها، کرم ها و تروجان ها حتما از نرم افزارهای اسکن اتوماتیک فلش مموری قبل از بکارگیری آن استفاده شود.

نرم افزارها

- کاربران تنها به منابع، برنامه ها و تنظیماتی که برای انجام کارهایشان لازم است، دسترسی دارند. شاید بعضی آن را محدودیت بدانند در حالیکه هدف محدود کردن کاربران نیست بلکه کاربر برای تمام کارهایی که باید انجام دهد دسترسی لازم را دارد و این محدودیت ظاهری هم برای کاربر و هم برای کل شبکه مفید است. به هر میزان که سطح دسترسی کاربر بالاتر از میزان ضروری برای انجام کارش برود، به همان میزان ریسک و خطر نفوذ و رخنه، ورود ویروس ها و کرم ها و از دست رفتن اطلاعات افزایش می یابد.
- امکاناتی از برنامه ها یا سیستم عامل که به آن احتیاج ندارید غیرفعال کنید.
- از دانلود کردن نرم افزارهای موجود در بازار یا اینترنت و نصب کپی نرم افزار ها (چه پرتابل و چه غیرآن) بر روی سیستم خودداری نموده و تنها از لیست برنامه های مورد تایید (موجود در FTP دانشگاه) استفاده نموده و درخواست نصب آن را از کارشناسان IT ننمایید. برخی نرم افزارهای غیراستاندارد، ابزارهای جاسوسی و برنامه های مخرب هستند که خود را در دل برنامه های کاربردی جای داده اند. برخی ابزارهای دانلود یا فیلترشکن ها از این دسته اند.
- همیشه از آخرین نسخه های نرم افزارها (مرورگرهای وب، نرم افزارهای کاربردی و ...) استفاده نمایید. چرا که در نسخه های جدید معمولا حفره های امنیتی نسخه های قدیمی برطرف می گردد.
- هنگام استفاده از وبسایت ها، به جهت تامین امنیت بیشتر ترجیحا از مرورگر Mozilla Firefox استفاده نمایید. (به جز در مواردی که وبسایت مذکور استفاده از Internet Explorer را به جهت استفاده از همه امکانات آن وبسایت توصیه نموده است.)
- هنگام استفاده از اینترنت از ابزارهای فیلترشکن مانند نرم افزارها یا پروکسی ها استفاده ننمایید. بدیهی است عواقب سو آن متوجه کاربر خواهد بود.

بررسی منظم امنیت کامپیوتر

- در بازه های زمانی مشخص وضعیت امنیتی سیستم کامپیوتری خود را مورد ارزیابی قرار دهید. انجام این کار در هر سال حداقل دو بار توصیه می شود.
- بررسی پیکربندی امنیتی نرم افزارهای مختلف شامل مرورگرها، نرم افزارهای سازمانی و حصول اطمینان از مناسب بودن تنظیمات سطوح امنیتی در این فرایند انجام می شوند.

نفوذ به روش های غیررایانه ای

گروهی از نفوذگران با استفاده از روش های غیر کامپیوتری و فنی و با کمک تکنیک‌های روانشناسی و هنرهای فردی خود، قربانیان اطلاعاتی را مورد حمله قرار می دهند. فرد مهاجم سعی می کند با استفاده از مهارت های اجتماعی خاص (نظیر روابط عمومی مناسب، ایجاد حس اعتماد، دوستی های مقطعی، حس انطباق پذیری کاذب، ظاهری آراسته و ...) ، با کاربران ارتباط برقرار نموده و با طرح سوالات متعدد و وادار نمودن آنها به ارائه اطلاعات (در حالیکه خود قربانی متوجه این مسئله نیست) ، بخش هایی از اطلاعات مورد نیاز خود به منظور نفوذ به اطلاعات سازمان یا رایانه شما را به دست آورد. در این روش تکنیک بکار گرفته شده توسط مهاجمین را «**مهندسی اجتماعی**» می نامند.

افراد مهاجم اطلاعات مورد نیاز خود را از طریق هم صحبتی با افراد پرحرف و زیاده گو، تخلیه تلفنی، اطلاعات مهم دور ریخته شده (ولی معدوم نشده) و نظایر آن به دست می آورند.

اقدامات لازم در صورت بروز حمله

- در صورتی که فکر می کنید به هر دلیلی اطلاعات حساس دانشگاه را در اختیار دیگران (افراد غیر مجاز) قرار داده اید ، بلافاصله موضوع را به اطلاع افراد ذیربط در دانشگاه (مثلا" مدیر شبکه) برسانید . آنان می توانند در خصوص هر گونه فعالیت های غیرمعمول و یا مشکوک، موضوع را بررسی کرده و ضمن اعلام هشدارهای لازم به دیگران مانع بروز بحران یا خسارت های بیشتر شوند.
- گزارشی در خصوص نوع تهاجم تهیه نموده و آن را در اختیار نهادهای مسئول در دانشگاه قرار دهید .
- ضمناً آگاه باشید هرگز دفاع در برابر حملات مهندسی اجتماعی نباید همراه با بی احترامی و یا پرخاشگری باشد، چرا که ممکن است در حین عصبانیت اقدام به افشای بخشی از اطلاعات مورد درخواست نفوذگر نمائید، همچنین این احتمال وجود دارد که در تشخیص مهاجم اشتباه کرده و شخص بی اطلاع از قوانین سازمان را با مهاجم اشتباه گرفته باشید. بنابراین در زمان قرار گرفتن در چنین شرایطی ضمن رعایت احترام با راهنمایی شخص متقاضی اطلاعات، وی را از قوانین مطلع کرده و راههای قانونی کسب اطلاعات مورد نیاز وی را به او نشان دهید.