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 فرایند نگاه کرد. بدون شک اطلاع رسانی در رابطه با تهدیدات حمل**ات و**نحوه برخورد با آنان دارای جایگاهی خاص در فرایند ایمن سازی اطلاعات بوده و لازم است نسبت به آخرین اطلاعات موجود در این زمینه خود رابروز نمائیم بدین دلیل وبا توجه به اهمیت اطلاع رسانی در این زمینه به اختصار مطالبی در ارتباط با امنیت اطلاعات هشدار های امنیتی ابزار های برخورد با حملات و تهدیدات امنیتی تقدیم می گردد.

ذخیره سازی جداگانه اطلاعات داده های مهم :

از هر نوع داده ارزشمند موجود بر روی یک کامپیوتر backup گرفته و انها را ذخیره نموده بدین ترتیب در صورتی که کامپیوتر سرقت و یا با مشگل مواجه شود امکان دستیابی به اطلاعات در معرض تهدید وجود خواهد داشت همنچنین از امکانات و دستگاه های متعددی به منظور ذخیره سازی داده میتوان استفاده نمود از جمله دیسک های فشرده cd,dvd یا فلش مموری ،هارد اکسترنال.

اطلاعات موجود بر روی دستگاه های قابل حمل (نظیر کامپیوتر های قابل حمل) بر روی رسانه های ذخیره سازی قابل حمل و در مکان های متفاوت ذخیره و نگهداری گردد. بدین ترتیب در صورت سرقت و یا خرابی یک کامپیوتر امکان دستیابی و اسفاده از داده ها همچنان وجود خواهد داشت.

رمز نگاری فایل ها:

با رمز نگاری فایل ها علی الخصوص فایل های حساس و دیتابیس های نرم افزار ها و سامانه های اداری مهم صرفا افراد مجاز قادر به دستیابی و مشاهده اطلاعات خواهند بود. در این صورت افراد غیر مجاز امکان دستیابی به داده ها را پیدا نمایند قادر به مشاده اطلاعات نخواهد بود.درزمان رمز نگاری اطلاعات میبایست تمهیدات لازم در خصوص حفاظت وبه خاطر سپردن رمز ها اتخاذ کردد.

طریقه استفاده صحیح از رمز های عبور:

سعی نمائید که برای استفاده از اطلاعات موجود بر روی دستگاه های کامپیوتری از جمله لبتاپ (فلش مموری،هارد اکسترنال،دیسک ها فشرده،و...) همواره از رمز عبور استفاده نمائید.

برای قرار دادن رمز عبور لطفا به نکات زیر توجه نمائید:

- حتما از حروف بزرگ و کوچک استفاده شود.

- حتما از سیمبلبه طور مثال: (@،!،#) استفاده شود.

- از گذاشتن تاریخ تولد ، کد ملی، نام خود واقوام جدا خودداری نمائید.

- از رمز های عبوری که امکان تشخیص آسان آن برای افراد غیر مجاز وجود دارد استفاده نکنید.

نحوه انتخاب و حفاظت رمز های عبور:

رمز های عبور روشی به منظور تائید کاربران بوده و تنها حافظ موجود بین کاربر و اطلاعات موجود بر روی یک کامپیوتر می باشد. مهاجمان با استفاده از برنامه های متعدد نرم افزاری،قادر به حدس رمز های عبور و یا اصلاحا crack نمودن آنان می باشد.

با انتخواب مناسب رمز های عبور و نگهداری آنان امکان حدس آنان مشگل و بالطبع افراد غیر مجاز به دستیابی اطلاعات شخصی شما نخواهند بود.

یکی از بهترین روشهای حفاظت از اطلاعات حصول اطمینان از این موضوع اشت که صرفا افراد مجاز قادر به دست یابی به اطلاعات می باشند، فرایند تائید هویت و اعتبار کاربران در دنیای مجازی شرایط و ویژگی های خاص خود را داشته و شاید بتواتن ادعا کرد که این موضوع به مراتب پیچیده تر از دنیای غیر مجازی است در صورتی که شما رمز های عبور را به درستی انتخواب نگرده و یا از آنان به درستی مراقبت ننمائید ،قطعا پتانسیل فوق جایگاه و کارایی واقعی خود را از دست خواهد داد.

تهداد زیادی از سیستم ها و سرویس ها صرفا به دلیل عدم ایمن بودنت رمز های عبور با مشگل مواجه شده و برخی ویروس ها با حدس و تشخیص رمز های عبور ضعیف توانسته اند به اهداف مخرب خود دست یابند.

چگونه یک رمز عبور خوب تعریف کنیم:

اکثر افراد رمز های عبوری استفاده می نمایند که مبتنی بر اطلاعات شخصی آنان است چرا که به خاطر سپردن این نوع رمز ها عبور برای آنان ساده تر می باشد بدیهی است به همین نسبت مهاجمان نیز با سادگی بیشتری به تشخیص و باز کردن رمز های عیور خواهند بود این نوع رمز های عبور دارای استعداد لازم برای حملات از نوع دیگشنری میباشد: (به منظور تعریف رمز عبور،موارد زیر پیشنهاد می گردد)

- عدم اسفاده از رمز های عبوری که مبتنی بر اطلاعات شخصی هستند زیرا این نوع رمزهای عبور به سادگی حدس و تشخیص داده می شوند.

- عدم استفاده از کلماتی که می توان آنان را به سادگی بتوان در اطراف سیستم مورد نظر پیدا کرد.

- از دادن رمز عبور خود به سایر افراد جدا خودداری فرمائید.

- از نوشتن رمز عبور بر روی کاغذ و گذاشتن آن بر روی میز محل کار نزدیک کامپیوتر و یا چسباندن آن بر روی کامپیوتر جدا اجتناب فرمائید.

- افرادی که امکان دستیابی فیزیکی به محل کار شما را دارند و میتوانند در زمان تایپ رمز عبور کیبورد را نگاه کنند به راحتی می توانند به رمز عبور شمنا دسترسی پیدا کنند لذا باید در هنگام تایپ رمز عبور مراقب چنین افرادی باشیم

- هرگز به خواسته افرادی که به بهانه های مختلف از طریق تلفن و یا نامه از شما درخواست رمز عبور را می نمایند توجه ننمائید.

- بسیاری از برنامه امکان به خاطر سپردن رمزهای عبور را ارائه می نمایند برخی از این برنامه دارای سطوح مناسب امنیتی به منظور حفاظت از اطلاعات نمی باشند.

- برخی برنامه ها (گوگل کروم، مازلا،اوپرا،و...)که با آنها سرویس ایمیل خود را چک میکنید اطلاعات را به صورت متن (غیر رمز شده) در یک فایل بر روی کامپیوتر ذخیره می نمایند این بدان معنی هست که افرادی که ب هکامپیوتر شما دستیابی دارند قادر به کشف تمامی رمزهای عبور و دستیابی به اطلاعاتشما خواهند بود. بدین دلیل همواره به خاطر داشته باشید زمانی که از یک کامپیوتر عمومی استفاده می نمائید حتما عمل logout را انجام دهید.

- برخی از برنامه ها از یک مدل رمز نگاری مناسب به منظور حفاظت اطلاعات استفاده می نمایند که ممکن است دارای امکانات ارزشمندی به منظور مدیریت رمزهای عبور باشند.

در ادامه به برخی موارد مهم و کاربردی اشاره می گردد:

- قفل نمودن کامپیوتر زمانی که از آن دور هستیم ،شما با قفل نمودن کامپیوتر خود عرصه را برای افرادی که با نشستن پشت کامپیوتر شما قصد دستیابی بدون محدودیت به اطلاعات شما قصد دستیابی بدون محدودیت به اطلاعات شما را دارند تنگ خواهید کرد.

-قطع ارتباط با اینترنت زمانی که از ان استفاده نمیگردد،پیاده سازی فناوری هایی نظیر dsl و مودم های کابلی پرسرعت این امکان را برای کاربران فراهم نموده است که همواره به اینترنت متصل و اصطلاحا online باشند. این مزیت دارای چالش های خاص خود نیز می باشد. با توجه به این که شما به طور دائم به شبکه اینترنت متصل میباشد مهاجمان و ویروس ها فرصت بیشتری برای یافتن قربانیان خود خواهند داشت.

- با توجه به تکنولوژِی فکر خوانی و رصد کاربران در فضای وب که بر اساس نوع وبگردی افراد و توسط موتور های قدرت مند جستوجو و تعدادی از نرم افزارها صورت میگیرد حتی الامکان قبل از عضویت در شبکه های اجتماعی و... از نام کاربری یوزرنیم و پسورد غیره و حتی پست های الکترونیک با عناوین دیگر استفاده نمود.

- از انجایی که مرورگرهای اینترنتی و نرم افزار های دیگر برای چک کردن مجوزهای امنیتی به تاریخ سیستم کاربر رجوع میکنند میبایست کاربران هر از چند گاهی تاریخ سیستم ومنطقه زمانی خود را برسی نمایند و از آن اطمینان حاصل کنند.

- جلوگیری از حملات فیشینگ،فیشینگ به تلاشی برای دستیابی به اطلاعات محرمانه کاربران مانند نام کاربردی کلمه عبور و اطلاعات کارت های اعتباری از طریق وارد نمودن وب سایت جعلی به عنوان وب سایت مورد اطمینان و شناخته شده گفته میشود

از روش های مقالبه با این حملات میتوان به موارد ذیل اشاره داشت:

*استفاده از مورور گرهایی که حاوی فهرستی به روز از سایت های جعلی بوده مانند مازیلا

*نظارت بر usb ها،usb ها مهمترین ابزار مهاجمین جهت انتقال الودگی به سیستمهای رایانه ای سازمان ها می باشند به منظور مقابله با نفوذ و انتشار بدافزار از طریق این رسانه ها می توان توصیه های زیر را در نظر داشت:

۱-دقت بیشتر در خصوص استفاده از رسانه های قابل حمل مشکوک به آلودگی و ناشناس

۲-اسکن و بررسی توسط آنتی ویروس معتبر پیش از استفاده از انها

۳- غیر فعال سازی دستی و دائمی خودکار این ابزار در سیستم

نصب و نگهداری نرم افزارهای آنتی ویروس:

- قفل نمودن کامپیوتر زمانی که از ان دور هستیم شما با قفل نمودن کامپیوتر خود عرصه رابرای افرادی که با نشستن پشت کامپیوتر شما قصد دستیابی بدون محدودیت به اطلاعات شما رو دارند را تنگ میکنید

- قطع ارتباط اینترنت زمانی که از آن استفاده نمیگردد درهنگام استفاده از فناوری هایی همچون adsl و مودم های کابلی این امکان را برای کاربران فراهم نموده است که همواره به اینترنت متصل و اصطلاحا online باشند این مزیت دارای چالش های امنیتی خاص خود نیز می باشد با توجه به این که شما به طور دائم به شبکه متصل میباشید محاجمان و ویروس ها فرصت بیشتری برای یافتن قربانیان خود خواهند داشت.

- حفاظت کامپیوتر ها در مقابل ویروس ها امری الزامی می باشد و می بایست همواره از به روز رسانی این نوع برنامه اطمینان حاصل نمود.

کارشناسان محترم فناری اطلاعات دانشگاه در سنوات اخیر نسبت به در اختیار قرار دادن نسخه های محتنلف آنتی ویروس و همچنین آپدیت روزانه آنها اقدام نمایند لیکن برخی کاربران نسبت به استفاده از این خدمات رایگان و آسان بی توجه می باشد.

نصب و نگهداری فایروال:

در صورت استفاده از شبکه های متعدد و پیچیده ضرورت استفاده از فایروال ها مضاعف میگردد،با استفاده از فایروال ها حفاظت نسبی و پیشگیری اولیه در خصوص دستیابی به سیستم توسط افراد غیر مجاز انجام خواهد شد.