Δ امنیت فیزیکی کامپیوترهای Laptop

حفـاظت

تعداد زیادی از کاربران ، خصوصا" افرادیکه مسافرت های متعدد تجاری و یا علمی را انجام می دهند ، از کامپیوترهای Laptop استفاده می نمایند . استفاده از این نـوع کامپیوترهـا ، بـه دلیـل کوچک بودن و حمل آسان به امری متداول تبدیل شده است . با توجه به گسترش استفاده ازکامپیوترهای فوق ، سارقین نیـز بـر روی این موضوع سرمایه گذاری کرده و برنامه ریزی لازم در خصوص سرقت آنان را انجام می دهند. (اهدافی جالب ، جذاب و چنـد منظـوره !) . تمـامی اسـتفاده کننـدگان کامپیوترهـای Laptop ، می بایست دقت لازم در خصوص حفاظت از ماشین و اطلاعات موجود بر روی آن را داشته باشند .

Δ 555555 تهدیدات 555555

صرفا" خود شما می توانید تشخیص دهید که با سرقت کامپیوتر ، چه چیزی در معرض تهدید قرار خواهـد گرفـت . اولـین موضـوع نگران کننده ، سرقت خود کامپیوتر است و در صورتی که سارق کامپیوتر ، قادر به دستیابی اطلاعات موجود بـر روی کـامپیوتر گردد ، تمامی اطلاعات در معرض تهدید قرار خواهند گرفت.افراد غیر مجاز، نمی بایست به اطلاعات مهم سازمانها و یـا اطلاعـات حساس مشتریان دستیابی پیدا نمایند . احتمالا" اخبار متعددی در خصوص نگرانی و هراس سازمان هائی را شنیده اید که برخـی از کامپیوترهای Laptop آنان گم و یا به سـرقت رفتـه اسـت . علت اصلی این همه نگرانی به وجود اطلاعات حسـاس و مهـم بـر روی اینگونه از کامپیوترها برمی گردد. حتی اگـر بـر روی آنـان، اطلاعات حساس سازمانی وجود نداشته باشـد ، سـایر اطلاعـات موجود در معـرض تهدیـد خواهنـد بـود . اطلاعـاتی نظیـر : قـرار ملاقات ها ، رمزهای عبور ، آدرس های Email و سایر اطلاعات مرتبط .

Δ توصیه هائی به منظور حفاظت کامپیوترهای Laptop

* ***حفاظت از کامپیوتر با استفاده از رمز عبور*** . پیشنهاد می گردد به منظور استفاده از کامپیوتر و Log in نمودن بـه آن از یـک رمز عبور استفاده شود .

***نگهداری کامپیوتر در تمامی مدت نزد خود** : در زمان مسافرت ، کامپیوتر Laptop را نزد خود نگهداری نمائید . در اغلب موارد ، سارقین به دنبال فرصت های مناسبی می باشند که بتواننـد بـه اهداف خـود نائـل گردنـد (بررسـی اطـاق هـای هتـل بـه منظـور دسترسی به کامپیوترهای بـی مراقـب) . در صـورتی کـه قصـد شرکت در یک همایش و یـا نمایشـگاه بازرگـانی را داریـد ، لازم است به این موضوع دقت شود که این نوع مکان ها شرایط مناسب و مطلوبی را برای سارقین فراهم می نمایند .

***کم اهمیـت جلـوه دادن داشـتن یـک کـامپیوتر Laptop.** ضرورتی ندارد که تبلیغ داشتن کامپیوتر Laptop خود را برای سـارقین انجـام دهیـد ! سـعی نمائیـد در مکـان هـای عمـومی از کامپیوترهای Laptop استفاده نکرده و برای جابجائی آنـان از کیف های سنتی استفاده نگردد .

***استفاده از یک قفل و یا دزدگیر** : تعداد زیادی از شرکت ها، قفل ها و یا دزدگیرهائی را ارائه نموده اند که می توان با تهیـه آنـان ، حفاظت کامپیوتر Laptop خود را افزایش داد . در صورتی کـه شما اغلب مسافرت می نمائید و یا در مکان های شلوغ مشغول به کار هستید ، می توانید از تجهیزات فوق بـه منظـور ایمـن سـازی کامپیوتر Laptop خود استفاده نمائید .

***گرفتن backup از فایل های موجـود بـر روی کـامپیوتر** . به منظور پیشگیری در خصوص از دست دادن اطلاعات ، پیشنهاد می گردد از اطلاعات مهم موجود بـر روی کـامپیوتر، Backup گرفته شده و آنان را در یـک مکـان جداگانـه ذخیـره نمائیـد . در چنین مواردی نه تنها شما قادر به دستیابی اطلاعات خواهید بود ، بلکه در صورت سرقت کامپیوتر ، امکان بررسی این موضوع کـه چه اطلاعاتی در معرض تهدید می باشند نیز وجود خواهد داشت .

Δ اقدامات لازم در صورت سرقت کامپیوتر

در صورتی که کامپیوتر laptop شما سرقت شده است ، مـی بایست در اسرع وقت موضوع را به اطلاع سـازمان هـای ذیـربط قانونی رسانده تا آنان مراحل و اقدامات لازم را انجـام دهنـد . در صورتی که بر روی کامپیوتر ، اطلاعات حسـاس سـازمانی و یـا اطلاعات مربوط به مشـتریان وجـود داشـته اسـت ، مـی بایسـت بلافاصله موضوع را بـه اطـلاع افـراد مسـئول در سـازمان خـود رسانده تا آنان سریعا" اقدامات لازم را انجام دهند .

Δ امنیت داده ها در کامپیوترهای قابل حمل

در زمان استفاده از دستگاه های قابل حملی نظیـر کامپیوترهـای Laptop عـلاوه بـر رعایـت اقـدامات احتیـاطی در خصـوص حفاظت فیزیکی آنان،می بایست یک لایه امنیتـی دیگـر بـه منظـور ایمن سازی داده ها را ایجاد نمود .

Δ چرا به یک لایه حفاظتی دیگر نیاز داریم ؟

بـه منظـور حفاظـت فیزیکـی کامپیوترهـای Laptop و سـایر دستگاه های قابل حمل از روش های متعددی استفاده می گـردد. استفاده از هر روشی بـه منظـور حفاظـت فیزیکـی، عـدم سـرقت اینگونه دستگاه هـا را تضـمین نمـی نمایـد . دسـتگاه هـای فـوق بگونه ای طراحی شده اند که امکان حمل و جابجـائی آنـان سـاده باشد و همین موضوع می تواند احتمـال سـرقت آنـان را افـزایش دهد . سرقت یک کـامپیوتر حـاوی اطلاعـات حسـاس پیامـدهای خطرناک امنیتی را بدنبال خواهد داشت . علاوه بر مـوارد فـوق ،

هر دستگاهی که به اینترنت متصل می گردد ، دارای استعداد لازم به منظور حملات شبکه ای متعددی است (خصوصا" اگر ارتباط از طریق یک اتصال بدون کابل ایجاد شده باشد).

Δعملیات لازم به منظور امنیت داده ها

استفاده صحیح از رمزهای عبور : سعی نمائید که برای استفاده از اطلاعات موجود بر روی دستگاه های قابل حمل همواره از رمزهای عبور استفاده نمائید . در زمان درج رمز عبور ، گزینه هائی را انتخاب ننمائید که به کامپیوتر امکان بخاطر سپردن رمزهای عبور را می دهد .از رمزهای عبوری که امکان تشخیص آسان آنان برای افراد غیرمجاز وجود دارد ، استفاده نگردد . از رمزهای عبور مختلفی برای برنامه های متفاوت استفاده نمائید

ذخیره سازی جداگانه داده های مهم :از امکانات و دستگاه های متعددی به منظور ذخیره سازی داده می توان استفاده نمود . فلاپی دیسک ها ، دیسک های فشرده CD، DVD و یا درایوهای فلش قابل حمل ، نمونه هائی در این زمینه می باشند . پیشنهاد می گردد اطلاعات موجود بر روی دستگاه های قابل حمل(نظیر کامپیوترهای Laptop) 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 کامپیوتر ، امکان دستیابی و استفاده از داده ها همچنان وجود خواهد داشت . مکان نگهداری داده ها می بایست دارای شرایط مطلوب امنیتی باشد.

رمزنگاری فایل ها : با رمزنگاری فایل ها ، صرفا" افراد مجاز قادر به دستیابی و مشاهده اطلاعات خواهند بود . در صورتی که افراد غیر مجاز امکان دستیابی به داده ها را پیدا نمایند ، قادر به مشاهده اطلاعات نخواهند بود. در زمان رمزنگاری اطلاعات ، می بایست تمهیدات لازم در خصوص حفاظت و بخاطر سپردن رمزهای عبور اتخاذ گردد . در صورت گم شدن رمزهای عبور، امکان دستیابی و استفاده از اطلاعات با مشکل مواجه می گردد .

نصب و نگهداری نرم افزارهای ضد ویروس : حفاظت کامپیوترهای قابل حمل در مقابل ویروس ها نظیر حفاظت سایر کامپیوترها بوده و می بایست همواره از بهنگام بودن این نوع برنامه ها ، اطمینان حاصل نمود .

نصب و نگهداری یک فایروال : در صورت استفاده از شبکه های متعدد ، ضرورت استفاده از فایروال ها مضاعف می گردد . با استفاده از فایروال ها حفاظت لازم و پیشگیری اولیه در خصوص دستیابی به سیستم توسط افراد غیرمجاز انجام خواهد شد

گرفتن داده ها Back up : از هر نوع داده ارزشمند موجود بر روی یک کامپیوتر می بایست back up گرفته و آنان را بر روی CD-ROM، DVD-ROM و یا شبکه ذخیره نمود. بدین ترتیب در صورتی که کامپیوتر سرقت و یا با مشکل خاصی مواجه شود ، امکان دستیابی به اطلاعات و تشخیص سریع داده های در معرض تهدید وجود خواهد داشت .

==========

پست الکترونیکی محل امنی برای اخبار و اطلاعات محرمانه نیست .

==========

امنیت فیزیکی کامپیوتر های lap tap

دفتر حراست دانشگاه با همکاری کانون بسیج جامعه پزشکی

برگرفته از سایت دانشگاه علوم پزشکی مشهد