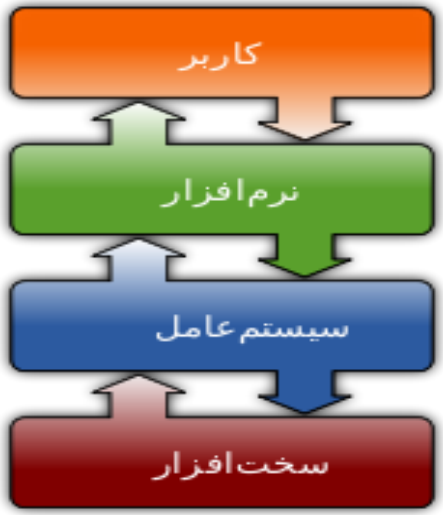
حفاظت از رایانه

در عصر دانش مهمترین وظیفه بشر جمع آوری داده ، ایجاد اطلاعات ، پردازش و رسیدن به دانش در زمینه های مختلف و در نهایت به اشتراک گذاشتن و تبادل دانش است. ولی استفاده از شبکه های کامپیوتری و همچنین اینترنت به عنوان ابزارهای اصلی برای این فرآیند ، با مخاطرات بسیاری همراه شده و امنیت داده ها را با چالشهای جدی مواجه نموده و به همین سبب حفظ امنیت و مدیریت داده های سازمانی در راس اهداف واحدهای فناوری اطلاعات سازمان ها قرار گرفته است.



تعریف امنیت شبکه

پردازه ایست که طی آن یک شبکه در مقابل انواع مختلف تهدیدات داخلی و خارجی امن میشود.

اهداف امنیت شبکه

(Security Center & Network Security):

۱ – ثابت کردن محرمانگی داده ها

۲ – نگهداری جامعیت داده ها

۳ – نگهداری در دسترس بودن داده ها

انواع تهدیدات به زبان ساده

۱ – کپی برداری غیر مجاز

۲ – ارسال اطلاعات

۳ – منتشر کردن اطلاعات

۴ – تغییر در ساختار ظاهری پایگاه

۵ – تخریب پایگاههای اطلاعاتی

۶ – ایجاد تغییر و دستکاری در اطلاعات

نکته: چیزی به اسم حفاظت صد در صد وجود ندارد. به همان تعداد که برنامه ها و قابلیتهایی برای ایمن سازی فایلها و پوشه ها وجود دارد ، به همان تعداد نیز دستورالعمل هایی برای کشف کلمات رمز وجود دارد.

اما روشهایی که در این مطلب به ان اشاره می شود ، اطلاعات شما را از گزند بیشتر تلاشها برای دستبرد حفظ می کند. اگر اطلاعات مورد نظر واقعاً اهمیت خاصی دارد ، استفاده از نرم افزارهای شناخته شده و معتبر پیشنهاد می شود.

چگونه مراقب رایانه و اطلاعات درون آنها و یا دسترسی غیرمجاز به منابع سیستم باشیم؟

الف) حفاظت فیزیکی

- اولین گام (حفاظت فیزیکی) از رایانه است. ایمنی در برابر سرقت و آتش سوزی و سیستم کنترل حریق باید به شکلی باشد که به نیروی انسانی و سیستم های الکترونیکی آسیب وارد نکند و همچنین موارد ناشی از نگهداری غیراستاندارد « وضعیت فیزیکی و محل پایه های سیستم ها و ...»
- باید کنترل کنیم که UPS (برق اضطراری) قدرت لازم را برای تامین نیروی الکتریکی جهت کارکرد صحیح سخت افزارها در زمان اضطراری داشته باشند.
- سیستم رایانه های شما از رطوبت و سرمایش استاندارد برخوردار باشد.
- تهیه یک نسخه پشتیبان از فعالیتهای روزانه و حفاظت از منابع ایجاد شده در خارج از سیستم جاری.

ب) حفاظت نرم افزاری

- قرار دادن Password مناسب در رایانه و فایلهای ذخیره شده و تغییر دوره ای آن.
- نصب یک نرم افزار ویروس یاب و به روز رسانی آن بطور مرتب.
- به روز رسانی مرتب سیستم عامل.
- نصب یک نرم افزار Firewall در صورت استفاده از اینترنت و شبکه.
- رعایت نکات ایمنی در هنگام استفاده از اینترنت و پست الکترونیک.

کامپیوتر شما از راههای زیر ویروسی می شود؟!

۱ – از طریق ایمیل (شایع ترین راه)

۲ – دریافت فایل از اینترنت یا از دوستان در شبکه های اجتماعی

۳ – استفاده از CD یا فلش حاوی ویروس

۴ – مشاهده صفحات وب در اینترنت

۵ – اجرای فایلهایDownloud شده از منابع بی اعتبار

راهکارهای پیشگیری از ویروسی شدن کامپیوتر شما

معمولاً روشهای زیر می باشد:

۱ – نصب ویروس یاب مطمئن (لاینسس دار) و به روز نگهداشتن آن.

۲ – باز نکردن ایمیل هایی که فرستنده آن را نمی شناسید.

۳ – امیل خود را از جایی تهیه کنید که سرویس دهنده ایمیل دارای ویروس یاب باشند(مثل Yahoo – Hot mail)

۴ – اکثر ایمیل های ویروسی به به سمت Spam ایمیل فرستاده میشود. لذا در باز کردن ایمیل های فرستاده شده به Spam دقت شود.

در صورت ابتلای کامپیوتر شما به ویروس چه باید کرد؟

۱ – اسکن (بازبینی) کل هارد توسط ویروس کشها.

۲ – تهیه یک نسخه پشتیبان از اطلاعات و نگهداری آن در CD

۳ – در صورت حاد بودن مشکل اگر امکان دارد ویندوز خود را عوض کنید و درایو ویندوز قبلی را فرمت نمایید.

نکات امنیتی در حفاظت رایانه

با فراهم شدن شبکه های رایانه ها و ورود این شبکه ها به زندگی شخصی و اجتماعی و سیستم های دولتی و شرکتهای خصوصی و همچنین ورود به دنیای ارتباطات می توان شاهد و نظاره گر انواع تهدیدات امنیتی در شبکه های رایانه ای باشیم.

۱ – اگر نامه شما دارای پیوستی با موضوع و عنوان مشکوک و یا غیرمنتظره می باشد، از باز کردن آن پرهیز نمایید. اگر می خواهید پیوست را باز کنید ابتدا آن را بر رایانه خود ثبت کنید و سپس توسط یک ضد ویروس معتبر آن را اسکن نمائید.

۲ – نامه های زنجیره ای و ناخواسته را پاک کنید. این دسته از نامه ها را هرزنامه می نامند زیرا بدون درخواست و در تعداد زیاد ارسال می گردد. هرزنامه ها را برای کسی نفرستید.

۳ – سرویسها و نرم افزارهایی که بصورت روزانه به آنها نیاز ندارید مانند (Remot Desktop ، File sharing services) را بر روی رایانه خود نصب نکنید. اینگونه سرویسها نقاطی هستند که می تواند درگاههای ورودی و نفوذ به رایانه شما باشد.

۴ – نرم افزارها و سیستم خود را در کمترین زمان بروزرسانی نمایید.

۵ – از اطلاعات و فایلهای مهم بصورت دوره ای ، کپی پشتیبان تهیه نموده و این کپی ها را بر روی CD و یا DVD و یا هر نوع منابع خارجی ذخیره کرده و در جای امن نگه دارید.

۶ – از برنامه های غیرقانونی که معمولاً بصورت رایگان در اینترنت ارائه میشود استفاده نکنید ، همین طور از برنامه های ارائه دهنده موسیقی و فیلم مجانی ، صرف نظر از غیرقانونی بودن آنها ، این برنامه ها معمولاً سرشار از انواع نرم افزارهای مخرب از جمله Spyware ها هستند.

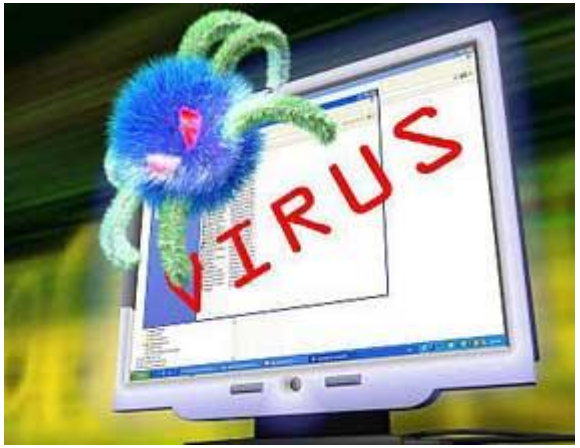
۷ – فرمت درایوها را به NTFS برای امنیت بیشتر تبدیل کنید.

۸ – سیستم های رایانه ای اداره صرفاً جهت انجام امور اداری می باشد بنابراین هرگونه نصب نرم افزار فقط با هماهنگی مسئول IT صورت پذیرید.

چگونه از

رایانه

خود محافظت کنیم؟



تهیه کننده: قائمیان – غفاری مقدم

شبکه بهداشت و درمان کلات

تابستان – ۹۴