امنیت اطلاعات

بخش دوم

ارائه شده در مرکز آموزش عالی علوم پزشکی وارستگان

مصطفی جهانگیر

مرداد ماه ۱۳۹۲

www.mjahangir.ir

mjahangir.blogfa.com

mjahangirf@gmail.com

امنیت حافظه فلش و هارد اکسترنال

حافظه های سیار و تهدیدات امنیتی آن ها

- **حافظه های سیار:**
  - حافظه های فلش دیسک ، کول دیسکها ، USB Flash– هارد خارجی (اکسترنال)
  - رم های دوربینهای فیلم برداری و عکس برداری (حافظه فلش دوربین)
- **تهدیدات حافظه های سیار:**
  - سرقت شدن حافظه توسط سارقان یا سرقت اطلاعات و دسترسی افراد غیر به اطلاعات
  - مفقود شدن (گم شدن)
  - آلوده شدن به ویروس ها
  - غیر قابل استفاده شدن کول دیسک توسط ویروس ها (در بسیاری از موارد مجبور به فرمت کردن فلش دیسک هستید و قادر به استفاده از اطلاعاتتان نخواهید بود .)

اقدامات امنیتی حافظه های سیار

- **گذاشتن پسورد بر روی حافظه های فلش دوربین**
  - بسیاری از دوربینهای عکس برداری و فیلم برداری این قابلیت را دارند که بر روی رم آنها پسورد بگذارید.
  - جهت دسترسی به این ویژگی به فایل راهنما و منوهای تنظیمات دوربین مراجعه نمائید.
- **استفاده از فلش دیسک فقط بر روی کامپیوترها و موبایل هایی که مجهز به نسخه های اصلی و معتبر آنتی ویروس هستند .**

اقدامات امنیتی حافظه های سیار

- Safe Remove کردن پیش از در آوردن کول دیسک از رابط USB و یا RAM Reader
  - با این شیوه پیش از قطع ارتباط فلش دیسک با کامپیوتر یا موبایل ، برق آن قطع شده و هنگام خارج شدن دچار مشکل و شوک نمی شود.
  - در مورد هارد دیسکهای خارجی عدم رعایت این مورد می تواند منجر به دست رفتن اطلاعات و حتی خراب شدن پارتیشن ها شود.
- پشتیبان گیری
  - وقتی اطلاعاتی را جهت انتقال بر روی فلش منتقل می کنید، نسخه اصلی که بر روی کامپیوتر می باشد را تا مدتی نگهداری کنید.
  - اطلاعات خود را می توانید بر روی سرویس های ذخیره سازی و پشتیبان گیری کلـود (ابری) ذخیره نمائید تا خیالتان آسوده باشد.

اقدامات امنیتی حافظه های سیار

- **از قرض دادن حافظه های فلش خود به دیگران خودداری کنید.**
  - اگر می خواهید حافظه و یا تجهیزات خود را با حافظه به دیگران مثلا تعمیرکاران بدهید، اطلاعات روی آن را با استفاده از Secure erase پاک نمائید.
- **هارد دیسکهای خارجی هنگام استفاده در یکجا ثابت باشند .**
  - توجه داشته باشید هارد دیسکهای خارجی هنوز به صورت مکانیکی هستند و هنگام اتصال آنها به کامپیوتر و مخصوصآ وقتی در حال رد و بدل کردن اطلاعات هستند باید در یک جا ثابت و بی حرکت باشند.
  - البته هارد دیسکهای خارجی نوت بوکی ویژگی هایی مانند ضد شوک دارند ، ولی ریسک از دست دادن اطلاعات در زمانی که هارد دیسک تکان می خورد بالاست.
  - حتی در زمانی که هارد از کامپیوتر جداست تکانها و شوکهای شدید به آن داده نشده و شرایط نگهداری هارد دیسکها مانند درجه حرارت و میزان رطوبت محیط را رعایت نمائید.

استفاده از سرویسهای ذخیره سازی ابری

- یکی از راه های ارسال فایل و اطلاعات برای دیگران استفاده از سرویسهای ذخیره سازی ابری است.
- سرویسهای ذخیره سازی ابری علاوه بر اینکه به شما امکان می دهند تا از فایلهای خود نسخه های پشتیبان بالادرنگ تهیه کنید و یا بر روی آنها اطلاعتتان را ذخیره کنید.
- می تواند فایل ذخیره شده بر روی سرویس کلـود را برای اشخاصی که در نظر دارید به اشتراک بگذارید.

امنیت بانکداری الکترونیک و پرداخت اینترنتی

سرویس های بانکداری اینترنتی

- امروز بسیاری از کاربران از سرویسهای اینترنت بانک (Internet Banking) برای مدیریت و نقل و انتقالات مالی خود بهره می گیرند و یا به صورت آنلاین اقدام به خرید کالا و خدمات می کنند .
- ولی همین کاربران به سادگی طعمه خلافکاران و دزدان سایبری شده و مشکلات بسیاری برای آنها به وجود می آید .

استفاده از وب سایت رسمی و معتبر بانکها

- حتماً تبادلات مالی را از وب سایت رسمی و اصلی بانکها و موسسات مالی انجام دهیم.
- تمام مراحل واریز هزینه و درج مشخصات کارت بانکی و پسوردها فقط در صفحه وب سایتی که لینک اصلی بانک می باشد صورت بپذیرد .
- در اختیار داشتن لینک پرداخت آنلاین نشان دهنده معتبر بودن آن وب سایت نیست.

استفاده از رایانه و موبایل شخصی

- برای ورود به اینترنت بانک و تبادلات مالی و بانکی فقط از سیستمها و رایانه ها و موبایل شخصی خود که به پاک بودن و ایمن بودن آنها اطمینان دارید استفاده کنید.
- استفاده از رایانه و موبایل دوستان ، اقوام و یا کافی نت ها که عموماً موارد ایمنی و امنیتی را رعایت نمی کنند با خطرات بسیاری همراه است و زمینه سوء استفاده از اطلاعات شخصی، مالی و بانکی شما را نیز مهیا می کند.

سایر موارد

- تعویض دوره ای پسوردها به ما کمک می کند تا از سلامت اطلاعات خود بیش از گذشته اطمینان داشته باشیم.
- همیشه پسورد POSرا خودتان وارد کرده و در نهایت فیش پول را بررسی نمائید تا از صحت هزینه کسر شده از حسابتان اطمینان حاصل کنید.

پیشگیری از حملات مهندسی اجتماعی و کلاهبرداری

یک حمله مهندسی اجتماعی چیست ؟

- به منظور تدارک و یا برنامه ریزی یک تهاجم از نوع حملات مهندسی اجتماعی ، یک مهاجم با برقراری ارتباط با کاربران و استفاده از مهارت های اجتماعی خاص (روابط عمومی مناسب ، ظاهری آراسته و ...)، سعی می نماید به اطلاعات حساس یک سازمان و یا کامپیوتر شما دستیابی و یا به آنان آسیب رساند.
- یک مهاجم ممکن است خود را به عنوان فردی متواضع و قابل احترام نشان دهد . مثلا" وانمود نماید که یک کارمند جدید است ، یک تعمیر کار است و یا یک محقق و حتی اطلاعات حساس و شخصی خود را به منظور تائید هویت خود به شما ارائه نماید.

نحوه پیشگیری از حملات مهندسی اجتماعی و کلاهبرداری

- به تلفن ها ، نامه های الکترونیکی و ملاقات هائی که عموما" ناخواسته بوده و در آنان از شما درخواست اطلاعاتی خاص در مورد کارکنان و یا سایر اطلاعات شخصی می گردد ، مشکوک بوده و با دیده سوء ظن به آنان نگاه کنید .
- در صورتی که یک فرد ناشناس ادعا می نماید که از یک سازمان معتبر است ، سعی نمائید با سازمان مورد ادعای وی تماس گرفته و نسبت به هویت وی کسب تکلیف کنید .
- هرگز اطلاعات شخصی و یا اطلاعات مربوط به سازمان خود را (مثلا" ساختار و یا شبکه ها) در اختیار دیگران قرار ندهید ، مگر این که اطمینان حاصل گردد که فرد متقاضی مجور لازم به منظور دستیابی به اطلاعات درخواستی را دارا می باشد .
- هرگز اطلاعات شخصی و یا مالی خود را در یک emailافشاء نکرده و به نامه های الکترونیکی ناخواسته ای که درخواست این نوع اطلاعات را از شما می نمایند ، پاسخ ندهید.

اقدامات لازم در صورت بروز تهاجم

- در صورتی که فکر می کنید اطلاعات مالی شما ممکن است در معرض تهدید قرار گرفته شده باشد ، بلافاصله با موسسه مالی خود تماس حاصل نموده و تمامی حساب های مالی در معرض تهدید را مسدود نمائید.
- گزارشی در خصوص نوع تهاجم را تهیه نموده و آن را در اختیار سازمان های ذیربط قانونی قرار دهید.

منابع

- DISNA - دیسنا – اولین پایگاه اطلاع رسانی *امنیت اطلاعات* ایران – *www.disna.ir/*
- ویکی پدیا – امنیت اطلاعات
- http://www.srco.ir/ – سایت سخاروش