مبانی امنیت در کامپیوتر و اینترنت

گردآوری و تنظیم: نکات کوچک

نکات کوچک www.tinytips.ir

فهرست مطالب

مقدمه

سخن کوتاهی پیش از آغاز مطالعه دوره آموزشی

در هر کار و شغلی که باشید نیازمند دانستن یک مبانی اولیه در مورد امنیت در کامپیوتر و دیگر ابزارهای دیجیتال هستید. ما در این فایل آموزشی این مبانی را به شما آموزش دهیم.

ممکن است با بعضی از آنها به خوبی آشنا باشید یا اینکه بیشتر مباحث برایتان جدید باشد. ما سعی کرده‌ایم که تمام موارد را تا حد امکان به زبان ساده و قابل فهم ارایه کنیم تا بتوانید حداکثر یادگیری را در این دوره داشته باشید.

هدف این است که بعد از پایان این دوره آموزشی به معنای واقعی و عملی، مبانی امنیت در کامپیوتر و اینترنت را فراگرفته باشید تا با اطمینان و امنیت بیشتری بتوانید از آنها استفاده کنید.

این دوره برای عمل کردن است نه فقط دانستن. اگر اصول و مبانی گفته شده را در عمل به کار نگیرید فایده‌ای به حال شما نخواهد داشت. بنابراین تمام نکات گفته شده را جدی بگیرید و سعی کنید با دقت و وسواس به آنها عمل کنید.

در بعضی درس‌ها نرم افزارهایی معرفی شده است. توصیه می‌شود همزمان با خواندن درس، عملا با این نرم افزارها کار کنید تا مهارت بیشتری پیدا کنید.

در اجرای آموزش‌های گفته شده دقیق باشید. شما آنها را با مسوولیت خودتان انجام می‌دهید. ما هیچ مسوولیتی را در قبال مشکلات احتمالی به عهده نمی‌گیرد.

درس اول – انتخاب رمز عبور مناسب و سوالات امنیتی

حریم خصوصی، واژه‌ای که با پیشرفت تکنولوژی تعریف جدیدی پیدا کرده است. واژه‌ای وسیع که حفظ آن هم دقت و معلومات خاص خود را می‌خواهد. حفظ حریم خصوصی و یا به تعبیر دیگر امنیت اطلاعات را از جنبه‌های مختلفی می‌توان بررسی کرد. اما اشتباه نکرده ایم اگر رمزهای عبور را سربازان خط مقدم مقابله با سارقان اطلاعات و هویت بنامیم. به همین خاطر است که اولین درس به این موضوع اختصاص یافته است. در ادامه به بایدها و نبایدها در انتخاب رمز عبور و نکات مهم در این مورد می پردازیم.

اجزای یک رمز عبور قوی

حتما این اصل ساده اما مهم را می دانید که یک رمزعبور باید به قدر کافی مشکل باشد تا یک برنامه کامپیوتری رمزشکن نتواند آن را به راحتی حدس بزند.

- رمزعبور باید طولانی باشد: رمزعبور هر چه طولانی تر باشد، احتمال اینکه یک برنامه کامپیوتری بتواند آن را حدس بزند کمتر می شود. سعی کنید رمز عبورتان حداقل ده حرف داشته باشد. البته بعضی افراد از رمزهایی شامل چند کلمه که با یا بدون فاصله پشت سر هم آورده می شوند، استفاده می کنند که اغلب به آنها عبارتِ رمز گفته می شود. ما نیز توصیه می کنیم تا آنجایی که برنامه یا سرویس مورد استفاده به شما اجازه می دهد، رمزعبور خود را طولانی انتخاب کنید.

- رمزعبور باید پیچیده باشد: علاوه بر طول، پیچیدگی نیز از کشف رمز توسط نرم افزارهای رمزشکن- که ترکیبی تصادفی از حروف را کنار یکدیگر قرار می دهند- جلوگیری می کند. پس در صورت امکان سعی کنید رمزعبور شما شامل حروف بزرگ انگلیسی، حروف کوچک انگلیسی، اعداد و علامت هایی مثل نقطه و کاما باشد. ضمنا یک رمزعبور می بایست به قدر کافی مشکل باشد تا افراد نتوانند آن را حدس بزنند.

- رمزعبور را باید بتوان به خاطر سپرد: اگر شما نتوانید رمزعبور خود را حفظ کنید و آن را جایی بنویسید، احتمالا آن را دو دستی به کسی که به خانه، کیف پول و یا حتی سطل آشغال دفتر شما دسترسی دارد، تقدیم کرده اید. راه های زیادی برای ایجاد و نگهداری رمزهای عبور

طولانی که بتوان آنها را حفظ کرد وجود دارد. اما امکان استفاده از نرم افزارهایی مثل «LastPass» که این کار را برای شما به خوبی انجام می دهند، نیز وجود دارد. البته استفاده از نرم افزارهایی مانند Microsoft Word برای این کار مناسب نیست. رمزعبور این فایل ها توسط نرم افزارهای رایگانی که در اینترنت نیز پیدا می شوند قابل بازیابی است. این مورد آنقدر اهمیت دارد که در یک درس مجزا به آن به طور کامل پرداخته شده است (درس آشنایی با نرم افزارهای مدیریت رمز عبور).

- رمزعبور نباید شخصی باشد: رمزعبور نباید هیچ ارتباطی با شخصیت شما داشته باشد، بنابراین از انتخاب کلمات یا عباراتی که قسمتی از اطلاعات شخصی شما هستند مانند نام، شماره کارت ملی، شماره تلفن ها، اسم فرزندان، روز تولد یا هر چیزی که ممکن است افراد دیگر درباره شما بدانند، پرهیز کنید.

- رمزعبورتان را مخفی نگه دارید: همیشه هنگام وارد کردن رمزعبور به افرادی که ممکن است آن را از روی شانه شما بخوانند توجه کنید. همچنین به جز در موارد کاملا ضروری رمزعبور خود را به هیچ کس نگویید. اگر هم مجبور بودید که آن را به دوست، هم کلاسی یا یکی از اعضای خانواده بگویید، ابتدا آن را به یک رمزعبور موقتی تغییر دهید و به شخص مورد نظر بدهید. پس از اتمام کار، آن را به حالت قبل بازگردانید. البته، اغلب اوقات راه های دیگری مانند ایجاد یک رمز عبور جداگانه در حساب خود وجود دارد که در صورت امکان بهتر است از این روش ها استفاده کنید. یک رمزعبور می بایست به گونه ای انتخاب گردد که اگر کسی آن را دانست، حداقل ضرر را برایتان به همراه داشته باشد.

- رمزهای عبور نباید یکسان باشند: از یک رمز عبور برای بیش از یک حساب استفاده نکنید، زیرا اگر کسی آن را بفهمد به تمام اطلاعات شما دسترسی پیدا خواهد کرد. فرض کنید رمزعبور کامپیوتر و ایمیل شما یکسان است، حال اگر کسی بتواند کامپیوتر شما را «هک» کند یا به طریقی رمز آن را بدست آورد، به ایمیل شما نیز دسترسی خواهد داشت.

- رمزهای عبور را به صورت دوره ای عوض کنید: توصیه می شود رمز عبور خود را به طور منظم حداقل هر ۳ ماه یک بار عوض کنید. زیرا به مرور زمان احتمال اینکه دیگران رمز عبور شما را

بفهمند، افزایش می یابد (طبیعی است اگر من رمزعبور خود را ۱۰ سال عوض نکنم به جز خواجه حافظ شیرازی، بقیه آن را خواهند فهمید). همچنین اگر کسی بدون اطلاع شما رمزعبورتان را دزدیده باشد تا زمانی که آن را عوض نکنید، از رمزعبور استفاده می کند.

چند راه خوب برای ساختن رمزهای عبور مطمئن

برای ساختن رمزعبور، بهتر است از کاراکترهای متنوع و روش های مختلف استفاده کنید. برای مثال:

- حروف بزرگ و کوچک: My naME is Not MR. MahMudi
- حروف و اعداد: a11 w0Rk 4nD N0 p14Y
- مخلوط کردن بعضی علامت ها: c@t(heR1nthery3
- استفاده از چند زبان: Let Them Eat 1e gateaU au ch()colaT (انگلیسی و فرانسه)

استفاده از این روش ها پیچیدگی و امنیت رمزعبور را بالا می برد، اما آن را کاملا بی معنی و غیر قابل حفظ کردن نمی کند. حتی استفاده از بعضی از راه های شایع مثل بکار بردن ۰ (صفر) به جای حرف O یا علامت @ به جای حرف a هم ایده خوبی است، زیرا این کار حداقل، زمان پیدا شدن رمز عبور توسط نرم افزار رمزشکن را افزایش می دهد یا آن را برای افراد معمولی غیر قابل حدس زدن می کند.

رمزهای عبور را می توان با علامت های جایگزین رایج (مثل مخفف ها) به عبارات پیچیده و عجیب تبدیل کرد. برای مثال:

«To be or not to be? That is the question» را می توان به صورت «Bon2B?TitQ۲» نوشت. یعنی به جای To عدد ۲ را که در زبان انگلیسی یکسان تلفظ می شوند را جایگزین می کنیم. یا مثلا به جای «That is the question» می نویسیم TitQ، یعنی حروف اول کلمات را کنار هم می آوریم. همان طور که می بینید عبارت اولیه ی معنی دار (بودن یا نبودن مسئله این است) را می‌توان به یک عبارت ظاهرا بی معنی تبدیل کرد.

مثال دیگر:

«We hold these truths to be self-evident: that all men are created equal» که با جایگزین کردن حروف اول هر کلمه (بعضی به صورت حروف بزرگ و بعضی کوچک) و قرار دادن نمادها به جای بعضی کلمات به جمله «WhtT2bs-e:taMac=» تبدیل می شود. مثال بعد: « Are you happy today?» تبدیل به «?rU:-)2d@y» می‌شود.

البته مثال های بالا مربوط به انگلیسی زبان ها است و برای ما راحت تر است که ابتدا جملات خود را به صورت فینگلیش بنویسیم و بعد روی آن تغییراتی را انجام بدهیم. کار بسیار ساده ای است: «من کتاب را خیلی دوست دارم» را می توان به صورت فینگلیش نوشت « man ketab ra kheili dust daram»: در این حالت می توان آن را هر جور که دوست دارید تغییر دهید؛ برای مثال «Mkrk2D@@r@m».

کار یک نرم افزار رمزشکن این است که حروف مختلف را با هم ترکیب کرده و آنها را در محل رمز عبور قرار می دهد تا از طریق آزمون و خطا، رمزعبور را بیابد. نویسندگان این برنامه ها می دانند که اکثر افراد از یک کلمه معنی دار برای رمزعبور خود استفاده می‌کنند، به همین دلیل برنامه خود را به گونه ای آماده می کنند تا ابتدا کلماتی را که در لغت نامه قرار دارد، امتحان کند. خب، نکته مثبت برای ما فارسی زبانان این است که اکثر این نرم افزارها برای زبان انگلیسی و لغات آن طراحی می شوند، پس توصیه می شود برای رمز عبور خود، به جای انگلیسی از فینگلیش استفاده کنید. البته راه عالی دیگری نیز وجود دارد. فرض کنید در حین وارد کردن رمز، کسی مخفیانه به کیبورد (صفحه کلید) شما نگاه می کند. اگر کلمه ای که شما می زنید یک کلمه‌ی انگلیسی یا فینگلیش باشد او به راحتی آن را متوجه می شود، چون معمولا افراد به حروف انگلیسی کیبورد توجه می کنند. اما انتخاب دیگری نیز پیش روی شماست، کلمه خود را فارسی تایپ کنید! احتمالا برای همه ما پیش آمده که می خواهیم در محلی یک کلمه فارسی بنویسم و بعد از اینکه آن را می نویسیم متوجه می شویم که زبان نوشته انگلیسی بوده و ما انگلیسی تایپ کرده ایم. مثلا ما در سایتی کلمه «محمد رضا گلزار!»

را می نویسیم اما چون حواس مان نبوده و زبان ویندوز را به فارسی تغییر نداده ایم این عبارت تایپ می شود «lpln vqh ‘gchv». به نظر شما این یک رمزعبور پیچیده نیست؟

در زیر مثال هایی از این روش را می آورم:

- بابا = fhfh
- میخوانمش = ldo,hkla
- رمزعالیجناب.سفید! = vlcuhgd[khf.stdn!
- من.یار/مهربانم۰داناوخوش.زبانم = lk.dhv/livfhkl0nhkh,o,a.cfhkl

در اینجا ما با توجه به حروف فارسی روی کلیدهای کیبورد کلمه فارسی مورد نظرمان را تایپ می کنیم، اما چون زبان سیستم عامل روی انگلیسی است، حروفی که در محل وارد کردن رمزعبور تایپ می شوند نیز انگلیسی خواهند بود. البته هنگامی که قرار بر استفاده از یک صفحه کلید بدون برچسب فارسی باشد (!) مساله بسیار سخت می شود.

این ها فقط چند راه ساده برای پیچیده کردن و در عین حال قابل حفظ ماندن رمزهای عبور هستند، بدیهی است که شما می توانید از روش‌های ابداعی خود برای این کار استفاده کنید.

سوالات امنیتی

در موارد زیادی در زمان ایجاد حساب کاربری مانند ثبت نام یک ایمیل جدید، شما امکان تعریف یک سوال امنیتی را دارید که در موارد خاص با پاسخ دادن به این سوال هویت خود را برای سرویس دهنده اثبات می کنید. این سوالات امنیتی اگر چه معمولا به چشم نمی آیند و برای انتخابشان وسواسی خرج نمی شود، اما از اهمیت بسیار بالایی برخوردارند. شاید هک شدن ایمیل یاهو خانم سارا پیلین (کاندید معاونت ریاست جمهوری آمریکا)، به دلیل ضعف در انتخاب سوال امنیتی، مثال خوبی برای نشان دادن اهمیت این سوالات باشد. خانم پیلن این سوال را انتخاب کرده بود: همسر خود را اولین بار کجا ملاقات کردی؟ هکر هم با حدس جواب این سوال توانسته بود به ایمیل ایشان نفوذ کند. حتی زمانی که شما درون گوگل به دنبال سوالات امنیتی مناسب می گردید در موارد زیادی

با نمونه های بسیار ضعیفی روبرو می شوید که استفاده از آن ها و موارد مشابه آن بسیار خطرناک است.

یک سوال امنیتی خوب باید این خصوصیات را داشته باشد:

۱. به راحتی به خاطر سپرده شود و یادآوری آن هم ساده باشد، به طوری که حتی طی ۱۰ تا ۱۵ سال آینده آن را فراموش نکنید.
۲. سوالی باشد که بتوان جواب های مختلفی را برای آن تصور کرد. سوالی با ۱۰۰۰ جواب ممکن که فقط یکی از آن ها درست باشد چطور است؟
۳. سوالی نباشد که در جاهایی مانند فیس بوک، کلوب، اورکات و امثال آن و یا در مصاحبه یا نظر سنجی به آن پاسخ داده باشید.
۴. جوابش در یک یا دو کلمه خلاصه شود.
۵. هرگز تغییر نکند (مثلاً نام دوست دختر/ پسر فعلی تان اصلا انتخاب مناسبی نیست!)

مواردی که به هیچ وجه انتخاب مناسبی نیستند:

۱. غذاهای مورد علاقه یا رنگ یا هر چیزی از علایق شخصی که در طول زمان تغییر می کنند.
۲. مدل و یا زمان ساخت اتومبیل تان، زیرا برای یک خوره ماشین، تشخیص مدل و سال ساخت آن از روی عکس اش چندان سخت نخواهد بود.
۳. تاریخ تولد: سوالات در این رابطه به دلیل سادگی یافتن جواب و وجود شبکه های اجتماعی مختلف که مرتبا تاریخ تولد شما را به همه یاد آوری می کنند غیر قابل استفاده اند.
۴. اسم و یا تاریخ تولد افراد خانواده: وقتی که افراد خانواده تان هم در شبکه های اجتماعی عضو هستند و در لیست دوستان تان هم قرار دارند، تنها کسی که مشخصات شناسنامه ای آنها را نمی داند خواجه حافظ شیرازی است.

۵. نام مدرسه و یا محل زندگی: پیدا کردن محل زندگی افراد و طبیعتا محل تحصیل آنها کار چندان دشواری نیست و به راحتی می‌توان چند احتمال قوی را مشخص و امتحان کرد.

۶. نام اولین شغل و یا نام موسسه ای که در آن مشغول شده اید: با کمی پرس و جو در خصوص محل تولد و زندگی تان، تنها تعداد محدودی شغل در لیست هکر محترم باقی می مانند که یک فرد می تواند به عنوان اولین کار انتخاب کند.

۷. سوالاتی از قبیل، چه رنگی است؟ رنگ های بسیار زیادی وجود دارد اما شما حتما یک رنگ مشخص از آن وسیله را دارید. به عنوان مثال: عکس ماشین تان در فیس بوک وجود دارد و همه از رنگِ آن مطلع هستند.

در پایین لیستی از سوالات خوب امنیتی با ذکر دلیل انتخاب آن ها آورده شده است:

۱. فامیل معلم کلاس سوم شما چیست؟ معمولا در مورد اسم معلم مدرسه با دیگران صحبت نمی کنیم و علاوه بر آن همه مدرسه‌های مختلفی را تجربه کرده ایم که تعداد زیادی معلم در مقاطع مختلف تدریس می کرده اند.

۲. برای دومین حیوان خانگی که داشته اید چه نامی انتخاب کرده بودید؟ اسم اولین حیوان خانگی شما در دسترس تر است، ولی این سوال را هم زمانی که هنوز دومین حیوان خود را نگهداری می کنید، انتخاب ننمایید.

۳. وقتی که بچه بودید، می خواستید در آینده چه کاره شوید؟ تنها زمانی از این سوال استفاده کنید که جواب شما مواردی مانند خلبان، آتش نشان، پلیس و از این قبیل موارد نزدیک به ذهن نباشد.

۴. اولین بار که خبر زلزله ی بم را شنیدید، کجا بودید؟ از جواب هایی مانند خانه، محل کار یا مدرسه خودداری کنید؛ البته این قبیل سوالات ناراحت کننده هستند ولی معمولا آن لحظات در ذهن ما باقی می مانند. هر واقعه ناگوار یا شادی آفرین فراموش ناشدنی را می توانید در اینجا استفاده کنید.

۵. زمان تحویل سال (مثلا ۱۳۶۵) کجا بودید؟ از آنجایی که در آن سال ها هنوز فیس بوک، تویتر، کلوب و حتی اینترنت هم وجود نداشته، معمولا در این باره اطلاعاتی وجود ندارد. اگر از شهرت زیادی برخوردار نیستید از این سوال استفاده کنید، فقط دقت کنید که در این تاریخ به دنیا آمده باشید!

۶. پسوند نام یا فامیل دوستان و آشنایان گزینه مناسبی به نظر می رسد. مثلا پسوند فامیل علی چیست؟ از آنجایی که حدس زدن هویت علی راحت نیست، این سوال انتخاب خوبی خواهد بود. ولی شما می توانید از سوالاتی مانند اسم گربه علی چیست؟ نیز استفاده کنید.

۷. قهرمان دوران کودکی شما که بود؟ شخصیت های زیادی می توانند قهرمان دوران کودکی باشند. این سوال بسیار مناسب است البته مشروط به اینکه پاسخش Superman یا اعضای خانواده تان نباشد.

۸. اسم کسی که پسوند فامیلش محسنی بود چیست؟ معمولا افراد از اسامی کامل خود برای معرفی (در شبکه های اجتماعی و یا ایمیل ها) استفاده نمی کنند و حدس جواب چنین سوالی بسیار مشکل است.

۹. نام دومین پسر/ دختری که عاشق اش شدید چه بود؟ البته حواستان باشد که این سوال را در صورتی انتخاب کنید که با او ازدواج نکرده باشید، زیرا یافتن نام همسرتان کار چندان مشکلی نخواهد بود! نام اولین معشوقه تان هم اصلا انتخاب مناسبی نیست، زیرا احتمالا آن قدر هیجان زده بوده اید که همه جا در مورد آن صحبت کرده اید!

۱۰. اولین بار کجا سیگار یا پیپ کشیده اید؟ این مورد معمولا در زمان نوجوانی شما اتفاق افتاده است و به نظرتان چنان محرمانه بوده که با هیچکس درباره آن صحبت نکرده اید!

مواردی هم وجود دارند که به نظر می رسد سوالات خوبی هستند در حالیکه واقعا اینطور نیست مانند:

۱. اسم مستعار دوران کودکی شما چه بود؟ این سوال خوبی نیست، زیرا افراد زیادی از دوستان و بستگان شما جواب آن را می دانند و احتمال دارد که خودتان در جایی به این سوال پاسخ داده باشید.

۲. اسم بزرگ ترین پسر عمو یا پسر خاله ی شما چیست؟ مثل اینکه باز هم از قدرت رسواگر شبکه های اجتماعی غافل شدید!

۳. تاریخ تولد برادر بزرگ شما؟

۴. ۵ رقم آخر شماره گواهینامه تان چیست؟

در آخر باز هم تاکید می کنیم، بسیاری از مواردی که در اینترنت به عنوان سوالات خوب امنیتی آورده شده اند، گزینه های خوبی نیستند و باید با اصول ذکر شده تطبیق داده شوند. فراموش نکنید که سوال های امنیتی مهم هستند و قبل از انتخاب آن ها خوب فکر کنید.

درس دوم – امنیت مرورگرهای اینترنتی

مرورگرها تبدیل به اصلی ترین نرم افزاری شده اند که در کامپیوتر از آن استفاده می کنیم و روز به روز هم جای بیشتری در میان کاربران باز می کنند. شما باید یک یا چند مرورگر را بسته به اینکه به چه امکانات و قابلیت هایی هنگام گشت و گذار در اینترنت نیاز دارید، انتخاب و از آنها استفاده کنید. اما نکته مهم، امنیت است. اینکه چه مرورگری امنیت بیشتری برای شما به ارمغان می آورد و رعایت چه نکاتی از طرف شما ضریب امنیتی تان را بالا می برد، مواردی است که در این درس، فرا خواهید گرفت.

چرا امنیت مرورگر مهم است؟

بیشترین درصد حملات و صدمات نرم افزاری و امنیتی که ممکن است متوجه یک کامپیوتر شود، از جانب اینترنت خواهد بود و در کنار آن بیشترین نرم افزارهایی که در یک سیستم با اینترنت در ارتباط هستند، مرورگرها هستند. بنابراین هکرها و افرادی که قصد کلاهبرداری های اینترنتی و یا آسیب رساندن به کامپیوترها را دارند، بیشترین تمرکز را بر روی مرورگرها می گذارند. پس لزوم استفاده از مرورگری مناسب و امن در کنار دقت و توجه به جزئیات، راز امنیت مرورگر، سیستم عامل و مهمتر از همه اطلاعات شما به حساب می آید.

چه مرورگری استفاده کنیم؟

نخستین و مهمترین مساله در رابطه با امنیت به هنگام مرور وب، انتخاب مرورگر است. هر کدام از مرورگرهای موجود، امکانات و قابلیت های خاصی را در اختیار کاربر قرار می دهند. اما مطمئنا مهمترین نکته برای بسیاری از افراد، امنیت است. در کنار آن باید فاکتورهای سرعت مناسب و قابلیت های کافی را نیز مد نظر قرار داد. پس در نهایت باید بسته به نیاز، مرورگری را انتخاب کرد که امنیت، سرعت و قابلیت های بیشتری را به نسبت سایر مرورگرها در اختیار ما قرار بدهد.

همه‌ی مرورگرها در رابطه با این سه فاکتور، نقاط قوت و ضعفی دارند. اما برای رفع چنین نیازهایی، مرورگرهای فایرفاکس، کروم و اُپرا، انتخاب هایی به مراتب بهتر از سایر مرورگرها به حساب می آید. هر چند ممکن است شما تا پیش از خواندن این درس فقط از اینترنت اکسپلورر استفاده کرده باشید، اما زمانش رسیده که مرورگرهای سریع تر و امن تری را هم امتحان کنید.

مرورگر فایرفاکس با سرعت مناسب و امکان نصب افزونه های مختلف، بهترین انتخاب برای افرادی است که امنیت را در کنار سرعت کافی و دسترسی به امکاناتی بی نهایت، می خواهند. اما در کنار آن مرورگر کروم، می تواند با ظاهری ساده تر و سرعتی به مراتب بیشتر، نیازهای کاربرانی که انتظار زیادی را از قابلیت های مرورگر خود نمی طلب اند، برآورده کند. مرورگر اُپرا نیز با سرعت مناسب و امنیت کافی، انتخاب خوبی برای افرادی است که ظاهری ساده و در عین حال آراسته را در کنار سرعت بالا، برای مرورگر خود می پسندند.

آشنایی با قسمت های مختلف مرورگر و توجه به جزئیات

در بسیاری از مرورگرها که ظاهری مشابه دارند، دو قسمت مهم وجود دارد که باید آنها را بشناسید: نوار بالا (Header Bar) و نوار وضعیت (Status Bar). توانایی شناسایی و همچنین توجه به این دو قسمت حین مرور صفحات وب، کمک شایانی به پیشگیری از بروز خطرات پیش رو، می کند. در قسمت بالای مرورگرها، دو نوار مختلف وجود دارد که Title Bar و Address Bar از مهمترین آنها به شمار می روند. در Title Bar که بالاترین قسمت پنجره اصلی مرورگر را شامل می شود، موضوع صفحه ای که در حال مرور آن توسط مرورگر هستید، نمایان می شود. در Address Bar نیز آدرس اصلی صفحه ای که در حال بازدید آن هستید، قابل رویت است. توجه به نوار آدرس یا Address Bar اهمیت ویژه ای دارد. همچنین آگاهی از وضعیت امنیتی و رمزگذاری صفحات وب با توجه به نوار آدرس امکان پذیر است.

در نوار پایین مرورگر، مهمترین قسمت Status bar یا نوار وضعیت قرار گرفته است. این نوار، اطلاعاتی از وضعیت مرورگر و لینک‌هایی که بر روی آنها کلیک می کنید نمایش می دهد. اگر در یک صفحه وب، نشانگر موس را بر روی یک لینک قرار دهید، می توانید آدرسی که لینک مورد نظر، شما را به آن ارجاع می دهد را در نوار وضعیت مرورگر مشاهده کنید. اهمیت این نوار بسیار زیاد است و توجه به آدرس اصلی لینک ها در تمامی صفحات وب، قبل از کلیک کردن‌شان، از اهمیت ویژه ای برخوردار است.

خطرات و راهکارها

کاربران باید برای پیشگیری از بروز خطراتی مانند فیشینگ، کلیک جکینگ و... تدابیری بیاندیشند. این موارد توسط برخی افراد و به منظور سرقت اطلاعات، کلاهبرداری و یا سوء استفاده از کاربران، ایجاد و به آنها تحمیل می شود و مهمترین راه مقابله، بالا بردن ضریب امنیتی مرورگر و دقت بیشتر کاربر است.

امنیت مرورگر چگونه تهدید می شود؟

مرورگرها برای افزایش قابلیت هایشان، وابسته به رابط های نرم افزاری مانند Flash و ActiveX و Java و Scripts (JavaScripts, VBScript,...) هستند. این تکنولوژی ها به صورت بالقوه می توانند به عنوان راه هایی برای دسترسی های غیرمجاز یا اجرای کدها و برنامه های مخرب باشند. در صورت انجام تنظیمات ناصحیح ممکن است خطرات امنیتی‌ای برای شما به وجود آید. برخی مرورگرها امکان غیر فعال سازی کامل این رابط های نرم افزاری را دارند. البته استفاده از افزونه هایی که به منظور مسدود کردن اسکریپت ها و کدهای اجرایی در مرورگر نیز تولید شده اند، راهی برای جلوگیری از اجرای خودکار آنها است.

همچنین پلاگین هایی مانند فلش پلیر (Flash Player) که وظیفه‌ی پخش فایل های فلش را دارند، بهتر است غیرفعال باشند اما اگر می خواهید از این پلاگین ها همچنان استفاده کنید باید اطمینان داشته باشید که آخرین نسخه از آنها روی کامپیوتر شما نصب است. در صورتی که از نسخه های قدیمی استفاده می کنید باید بدانید که در معرض خطرات جدی امنیتی هستید.

استفاده از افزونه های امنیتی

اکثر مرورگرها افزونه هایی دارند که برای سرعت بخشیدن به کارها و یا اضافه شدن قابلیتی، بر روی آنها نصب می شود. اما افزونه هایی نیز هستند که برای بالا بردن ضریب امنیتی مرورگر، بهتر است نصب شوند. در این میان بیشترین تعداد افزونه‌های امنیتی متعلق به فایرفاکس است. برای یک وبگردی امن تر استفاده از این افزونه ها بر روی فایرفاکس توصیه می شود:

افزونه: NoScript

بعضی کاربران اینترنت تصور می کنند که خیلی حواسشان به امنیت کامپیوترشان است. شما یک آنتی ویروس قوی نصب می کنید و هر چند ساعت یک بار آن را به روز می کنید، سیستم عامل مرتب آپدیت می شود، انواع و اقسام آنتی اسپای (Anti-spy) دارید، یک فایر وال (Firewall) قوی نصب کرده اید و خلاصه هر نوع چفت و بندی را برای کامپیوترتان ایجاد می کنید. اما بعد از این همه کار، هنگام گشت و گذار در وب مثل آب خوردن هک می شوید! علت این است که وقتی از یک صفحه وب بازدید می کنید، بعضی کد ها مثلا کدهای جاوا اسکریپت، فلش، جاوا و... بر روی کامپیوتر شما اجرا می شوند. این کدها قادراند که به صورت بالقوه به کامپیوتر شما آسیب برسانند و یک هکر از طریق آنها می تواند به کامپیوتر شما نفوذ کرده یا با یک حمله که XSS نام دارد حساب های اینترنتی شما را مانند ایمیل و... سرقت کند.

متاسفانه در اینترنت تشخیص امن بودن یا خطرناک بودن یک وب سایت، کار آسانی نیست. شما از روی شکل ظاهری یک صفحه اینترنتی نمی توانید حدس بزنید که چه خطری کامپیوترتان را تهدید می کند. خیلی اوقات با استفاده از موتورهای جستجو وارد سایت هایی می شوید که تا به حال اسمشان را هم نشنیده اید و یا از طریق ایمیل لینک هایی دریافت می کنید که با کلیک کردن روی آنها به صفحاتی وارد می شوید که معلوم نیست چه چیزی در آنها پنهان شده است.

این افزونه یک کار ساده اما بسیار مهم انجام می دهد و آن غیرفعال کردن کدهایی است که امکان آسیب رساندن به کامپیوتر شما را داشته باشند. کدهایی مانند جاوا اسکریپت، فلش، جاوا و یا هر کد اجرایی دیگر که روی مرورگر شما اجرا می شود.

شاید پیش خود بگویید که خیلی از سایت ها برای اینکه درست نمایش داده شوند نیاز به اجرای جاوا اسکریپت و فلش دارند. با استفاده از این پلاگین احتمالا در مشاهده بسیاری از سایت ها به مشکل بر خواهم خورد. پاسخ این سوال هم مثبت است و هم منفی.

این افزونه به شما اجازه می دهد که امکان اجرا شدن کدهای جاوا اسکریپت و فلش را برای هر سایت به صورت مجزا تعیین کنید. در واقع می توانید یک لیست مجاز از سایت های مورد اعتماد خودتان ایجاد کنید و تنها به این سایت ها اجازه دهید تا جاوا اسکریپت یا فلش را بر روی مرورگر شما اجرا

کنند؛ و به بقیه سایت ها چنین اجازه ای ندهید. در مورد سایت های ناشناس و سایت های عبوری دلیلی وجود ندارد که اجازه اجرای هر کدی به آنها داده شود چرا که در این صورت امنیت کامپیوتر شما به شدت به خطر می افتد.

استفاده از این پلاگین آسان است، کافیست که همیشه یک اصل را در ذهن داشته باشید: شما فقط در مواردی که واقعا به سایتی اعتماد دارید و نیاز به فعال کردن فلش یا جاوا اسکریپت وجود دارد به آنها اجازه فعالیت می دهید. در غیر این صورت نیازی به اجازه دادن برای فعال شدن آنها نیست.

ممکن است در ابتدا استفاده از این افزونه مقداری آزاردهنده به نظر برسد. چرا که در ابتدای استفاده مجبور هستید تعدادی از سایت های مورد اعتمادتان را به آن معرفی کنید تا به آنها اجازه کارکرد صحیح را بدهد. اما باید بدانید که حملات XSS یکی از خطرناک ترین و شایع ترین روش های حمله و سرقت اطلاعات در اینترنت است و هیچ کدام از روش های مقابله ای که تا به حال استفاده می کردید قادر به جلوگیری از آنها نیست. این افزونه یکی از معدود روش هایی است که می تواند تا حد زیادی جلوی این حملات را بگیرد و امنیتی بسیار بیشتر از گذشته به شما هدیه کند.

افزونه: AdBlockPlus

وقتی در اینترنت وب گردی می کنید، به سایت های مختلفی سر می زنید. معمولا به هر سایتی هم که مراجعه می کنید تعداد زیادی تبلیغ وجود دارد که مجبورید آنها را ببینید. اما آیا راهی وجود دارد که از شر تبلیغات داخل وب سایت ها خلاص شویم؟

ابتدا باید در مورد این موضوع فکر کنیم که چرا نمی خواهیم تبلیغات سایت ها را ببینیم؟ یک دلیل مهم به خصوص با این سرعت کم اینترنت در ایران، بالا بردن سرعت باز شدن صفحات و صرفه جویی در مصرف پهنای باند است. قسمت مهمی از حجم صفحه ای که باز می کنید را تبلیغات درون آن تشکیل داده است. حالا اگر راهی پیدا کنید تا جلوی بارگذاری (لود) شدن آنها را بگیرید، سرعت باز شدن این صفحات بهتر خواهد شد.

دلیل دیگر شاید این باشد که برخی تبلیغات سایت های ناشناس به سایت های کلاهبرداری و کدهای مخرب منتهی می شوند. اگر جلوی لود شدن این تبلیغات را بگیرید به بالا بردن امنیت خودتان هم

کمک کرده اید و آخرین دلیل شاید این باشد که از دیدن تبلیغات مزاحم در بعضی سایت ها که خودشان را با انبوهی از بنرها خفه کرده اند، خسته شده اید و دوست دارید اصل مطلب را ببینید.

اما راه حل چیست؟

پاسخ بسیار ساده است؛ اگر کاربر مرورگر فایرفاکس هستید، با نصب یک افزونه به نام Adblock Plus می توانید از دست بیشتر تبلیغات اینترنتی خلاص شوید. کافی است به صفحه نصب این افزونه بروید و با یک کلیک آن را نصب کنید و یک بار مرورگر را ری استارت کنید.

بعد از آن هیچ کار اضافه ای نباید انجام بدهید. خود این افزونه به صورت هوشمند تبلیغات درون سایت ها را شناسایی می کند و جلوی بارگذاری آنها را می گیرد. شما در عمل نیاز به انجام هیچ کاری ندارید. علامت این افزونه هم در بالای مرورگر شما ظاهر می شود.

وقتی روی حالت قرمز رنگ قرار گرفته باشد، یعنی جلوی لود تبلیغات سایت را گرفته است. اگر می خواهید به سایتی اجازه دهید که تبلیغاتش را لود کند کافی است وقتی که به آن سایت سر می زنید، بر روی علامت این افزونه کلیک کنید و اجازه‌ی فعال شدن تبلیغات در آن سایت را بدهید. در این حالت رنگ آیکون افزونه برای این سایت به حالت سبز در می آید.

اگر کاربر مرورگر کروم هستید، باید بدانید که خوشبختانه این افزونه برای این مرورگر هم وجود دارد و می توانید آن را بر روی کروم هم نصب کنید و از وب بدون تبلیغات لذت ببرید.

افزونه: Https Everywhere

آیا می دانستید که بسیاری از سایت ها، به شما این امکان را می دهند که برای امنیت بیشتر به صورت امن و به حالت اس اس ال (SSL) به آنها متصل شوید تا اطلاعات شما در مسیر دیده نشوند، اما از آنها اطلاع ندارید؟

برای استفاده از این امکان تنها کافی است افزونه‌ی Https Everywhere را بر روی فایرفاکس یا مرورگر کروم نصب کنید. بعد از آن تمام سرویس هایی که امکان اس اس ال روی آنها فراهم است، به صورت پیش فرض روی این حالت باز می شوند. تمام جستجوهای گوگل روی حالت اچ تی تی پی اس

(Https) خواهد بود. حتی سایت روزنامه نیویورک تایمز و ویکی‌پدیا هم به صورت اس اس ال ارایه می شوند، که در صورت نصب این افزونه آنها را هم در حالت اچ تی تی پی اس خواهید دید.

لینک دانلود این افزونه برای مرورگرهای گوناگون

شناسایی لینک ها و صفحات مشکوک

همه‌ی مرورگرهای اینترنتی، دو قسمت بسیار مهم دارند، که حین گشت و گذار در وب، باید بسیار مورد توجه قرار گیرند: Address Bar وStatus Bar. کاربر قبل از کلیک روی یک لینک و همچنین قبل از پر کردن فیلدهای صفحات لاگین در حساب های ایمیل و پروفایل های خود، باید این دو قسمت را زیر نظر بگیرد. در ابتدای درس هم در این مورد صحبت کردیم.

به هنگام کلیک بر روی یک لینک، در صورتی که نشانگر موس بر روی لینک مورد نظر نگه داشته شود، لینک اصلی آن در قسمت پایین مرورگر (Status Bar) نمایان می شود. با توجه به توضیحات لینک و آدرس URL می توان تا حد زیادی نسبت به سالم یا مشکوک بودن آن، تصمیم گیری کرد. توجه به این مورد، می تواند کاربر را در موارد زیادی از شر صفحات خطرناک و یا مشکوک، حفظ و از مشکلاتی که ممکن است برای او به وجود آید، ایمن کند.

همچنین هر کاربر، قبل از اینکه در سایتی لاگین کند، باید آدرس مربوط به آن را چک کند. برای مثال در صورتی که قصد ورود به ایمیل یاهو را داشته باشد، با اینکه صفحه باز شده بسیار شبیه صفحه لاگین در ایمیل یاهو است، آدرس صفحه مورد نظر را در Address Bar مرورگر بررسی کند تا آدرس سایت دیگری در آن قرار نگرفته باشد. این آدرس باید دامین یا یکی از زیر دامنه های سایت یاهو باشد. چنانچه آدرس مربوطه با آدرس سایت یاهو تطابق نداشته و فرد اقدام به لاگین نماید، حتی اگر پس از لاگین موفق به ورود به ایمیل خود شود، احتمالا قربانی فیشینگ شده، نام کاربری و رمزعبور خود را به هکر تحویل داده است! پس دقت در این مورد اهمیت بسیاری دارد.

استفاده از مرورگر برای نگهداری رمزهای عبور، بله یا خیر؟

همانطور که اشاره شد، مرورگرها عمده ترین و نخستین هدف هکرها برای دسترسی به اطلاعات کاربران و کلاهبرداری از آنها هستند. با وجود اینکه ممکن است کاربر مرور صفحات وب را با توجه به اقدامات و استفاده از افزونه ها، با امنیت تمام انجام دهد، اما استفاده از مرورگر برای نگهداری از

رمزهای عبور به هیچ وجه توصیه نمی شود. همانطور که در درس مدیریت رمزهای عبور گفته شد، بهتر است برای این منظور از نرم افزارهای مدیریت رمزهای عبور قدرتمندتر مانند LastPass استفاده شود.

پاک کردن تاریخچه مرورگر، Cache و کوکی ها

هر بار که از مرورگر خود استفاده می کنید، بسته به اینکه از چه سایت هایی بازدید کرده باشید، تاریخچه مرورگر و اطلاعاتی از سایت مورد نظر در کامپیوتر شما ذخیره می شود. بهتر است جهت افزایش امنیت، این اطلاعات پس از مدتی کوتاه پاک شوند. می توانید مرورگر خود را طوری تنظیم کنید که این فایل ها و اطلاعات پس از هر بار بستن مرورگر، به صورت خودکار از کامپیوتر شما پاک شوند.

Private Browsing Mode

در صورتی که بخواهید سایتی را مرور کنید که پس از آن هیچ ردپایی از شما در مرورگر و کامپیوتر باقی نماند، استفاده از Private Browsing Mode توصیه می شود. برخی مرورگرها همانند فایرفاکس و کروم از قابلیت Private Browsing پشتیبانی می کنند. نام این حالت در مرورگر کروم Incognito است. می توانید برای حفظ حریم خصوصی از این حالت برای مرور سایت ها استفاده کنید. در حالت Private Browsing صفحات بازدید شده، اطلاعات ورودی در فرم ها و فیلدهای جستجو، رمزهای عبور، کوکی ها و کش صفحات ذخیره نمی شود. پس هیچ ردپایی از شما در کامپیوتر باقی نمی ماند.
برای استفاده از این حالت در فایرفاکس می توانید در منوی Tools بر روی Start Private Browsing کلیک کنید. به هنگام مرور وب در این حالت، در Title Bar مرورگر عبارت Private Browsing ظاهر می شود.

به روز رسانی مرورگر و افزونه ها

همانطور که در ابتدای این درس اشاره شد، مرورگرها به این دلیل که بیشترین نقطه‌ی اتصال بین کامپیوتر و دنیای خارج هستند، همواره خطری بالقوه محسوب می شوند. چرا که هکرها از حفره های امنیتی مرورگرهای مختلف در جهت نفوذ به کامپیوتر کاربران استفاده می کنند. اما توسعه دهندگان مرورگرهای اینترنتی به صورت متناوب در حال به روز رسانی مرورگرها و رفع حفره ها و باگ های امنیتی این نرم افزارها هستند، به همین دلیل یکی از مهمترین عوامل در جلوگیری از سوء

استفاده‌های احتمالی هکرها، به روز رسانی منظم مرورگر است. پس این نکته را جدی بگیرید و در صورتی که نسخه جدیدی از مرورگر مورد استفاده شما عرضه شد، در اولین فرصت نسبت به آپدیت مرورگرتان اقدام کنید.

در رابطه با به روز رسانی مرتب افزونه های مرورگر خود نیز منظم باشید، چرا که ممکن است استفاده از نسخه های قدیمی و به روز نشده برخی افزونه ها نیز خطراتی به شما تحمیل کنند. البته توصیه می شود تنها افزونه هایی که بیشتر مورد استفاده قرار می دهید، بر روی مرورگر خود نصب نمایید و از نصب افزونه های اضافی خودداری کنید. این امر علاوه بر افزایش سرعت مرورگر، موجب افزایش ضریب امنیتی آن و در نهایت کامپیوتر شما نیز می شود.

مرورگر فایر فاکس امکان جالبی را در اختیار کاربرانش قرار داده که می توانند از به روز بودن پلاگین هایشان اطمینان حاصل کنند. کافی است به این صفحه سر بزنید تا از به روز بودن پلاگین ها اطمینان حاصل کنید. در صورتی که همه پلاگین ها به صورت سبز رنگ نیستند، بدانید که باید فورا آنها را آپدیت کنید.

درس سوم – امنیت ایمیل و چت

عمده ارتباط افراد در اینترنت بر پایه ایمیل و چت پایه ریزی شده است. روزانه بسیاری از افراد از طریق این دو راه ارتباطی، اقدام به مکاتبه یا مکالمه می کنند. اما چنانچه نکات امنیتی در این ارتباطات رعایت نشود، ارسال یک ایمیل و چت در حالت معمولی و بدون توجه به اصول امنیتی، با ارسال یک نامه معمولی و یا یک تلفن غیر امن، قابل مقایسه است. در این درس با توجه به اهمیت امنیت در این ارتباطات، به دلایل و روش های بالا بردن ضریب امنیتی در این ابزارهای ارتباطی می پردازیم.

امنیت در ایمیل

ارتباطات رسمی و حتی غیر رسمی بسیاری از افراد از طریق ایمیل برقرار می شود. نکاتی از جمله انتخاب رمز عبور مناسب برای آدرس ایمیل، از نکات اولیه‌ی محافظت از ایمیل و جلوگیری از دسترسی های غیرمجاز به صندوق پست الکترونیکی به شمار می رود. لازم است رمز عبور ایمیل خود را حداقل سالی دو بار عوض کنید. تعویض رمز عبور را با ترکیبی از حروف، اعداد و علامت های خاص انجام دهید و هرگز از کلماتی که در فرهنگ های لغت موجود هستند، برای رمزعبور خود استفاده نکنید. همچنین در کنار آن لازم است از عدم وجود جاسوس افزارها، تروجان و سایر بدافزارهای احتمالی که می توانند اطلاعات ما را به یغما ببرند، مطمئن شوید. اسکن سیستم توسط نرم افزارهای ضد جاسوس افزار و ضد ویروس، برای اطمینان از این مورد توصیه می شود. توجه کنید که در مورد تمام این موارد در همین دوره به طور مفصل صحبت شده است.

افراد بسیاری از سرویس های رایگان ایمیل شرکت های بزرگی همچون یاهو، گوگل و مایکروسافت استفاده می کنند. اما توصیه می شود جهت امنیت بیشتر پست الکترونیکی تان از سرویسی استفاده کنید که از SSL بهره می برد. بدین منظور از جیمیل (Gmail) که سرویس ایمیل شرکت گوگل است، استفاده شود. این سرویس، امنیتی به مراتب بیشتر از سایر سرویس های پست الکترونیکی دارد، چرا که همواره از SSL برای برقراری ارتباط استفاده می کند.

برای اینکه مطمئن شوید سرویسی که از آن استفاده می کنید از SSL برای برقراری ارتباطات رمزگذاری شده و امن، بهره می برد، هنگامی که صندوق پست الکترونیکی خود را باز می کنید به

قسمت Address Bar مرورگر خود توجه کنید. چنانچه آدرس صفحه مربوطه با https شروع شود، سرویس مربوطه از ارتباط امن بهره می برد.

دقت کنید که لازم است صفحه ورود به صندوق پست الکترونیک شما نیز مبتنی بر https و رمزگذاری شده باشد. بدین ترتیب از رمز عبور شما نیز حفاظت می شود.

SSL اطلاعات صفحه را بین مبدا و مقصد رمزنگاری کرده و از دسترسی های غیر مجاز در میانه راه جلوگیری می کند. در رابطه با پست الکترونیکی نیز، در صورتی که سرویس ایمیل مربوطه فاقد SSL باشد، این امکان وجود دارد که اطلاعات رد و بدل شده در میانه راه توسط افراد غیر مجاز که در مراکز انتقال داده هستند، قابل دسترس شود. استفاده از SSL باعث می شود که ایمیل های ارسالی و دریافتی قبل از اینکه از کامپیوتر مبدا خارج شوند، کد شده و تنها در مقصد قابل خواندن باشند.

جیمیل بصورت خودکار روی https تنظیم شده است.

اهمیت به روز رسانی سیستم عامل، مرورگر و نرم افزاهای مورد استفاده

برای اطمینان از امنیت ایمیل، به روز رسانی مرتب و مکرر سیستم عامل، مرورگر و نرم افزارهای مورد استفاده در سیستم اهمیت ویژه ای دارند. بسته های به روز رسانی معمولا آخرین حفره های امنیتی نرم افزارها را پوشش می دهند و از سوء استفاده هکرها از این اشکالات پیشگیری می کنند. به همین جهت لازم است در جهت افزایش امنیت ایمیل از به روز بودن کامپیوتر، اطمینان حاصل کرد. به روز رسانی افزونه های مورد استفاده در مرورگر و نرم افزارهایی همچون جاوا، فلش پلیر و ادوبی ریدر نیز از این قاعده مستثنا نیست.

کلاینت های ایمیل

علاوه بر وب میل که راهی برای دسترسی به صندوق پست الکترونیکی است، استفاده از POP3 و IMAP نیز برای برقراری ارتباط با صندوق پست الکترونیکی و دریافت و ارسال ایمیل شایع است. برای استفاده از این دو پروتکل کلاینت هایی همچون Outlook و Thunderbird و... مورد استفاده قرار می گیرند.

کلاینتی را انتخاب کنید که در کنار امنیت و قابلیت های مفید، کار با آن راحت بوده و در دسترس باشد. در صورتی که می خواهید برای چک کردن ایمیل از کلاینت استفاده کنید، توصیه می شود تاندربرد را انتخاب نمایید.

این نرم افزار محصولی از شرکت موزیلا است و با قابلیت های بالا و افزونه های امنیتی متعدد، امنیت ایمیل شما را همانند وب میل تضمین می کند. افزونه های EnigMail و GnuPG برای افزایش ضریب امنیتی و بالابردن امنیت حریم ایمیل شما به هنگام استفاده از تاندربرد، توصیه می شوند.

تفاوت POP3 و IMAP در نوع ارتباط با سرور است. در POP3، کلاینت ایمیل های جدید را بر روی کامپیوتر دانلود می کند و کاربر می تواند بدون ارتباط مستقیم با سرور، ایمیل ها را مطالعه کند؛ اما در IMAP ارتباط با سرور به صورت مستقیم است و ایمیل ها، به صورت بی درنگ به کلاینت سرازیر می شوند. همچنین اگر ایمیلی در کلاینت خوانده شود، در صورت برقراری ارتباط با استفاده از IMAP، ایمیل مربوطه در وب میل و سایر کلاینت هایی که به آن آدرس ایمیل دسترسی دارند، «خوانده شده» می شود. قابلیت همزمان سازی در IMAP برای کاربرانی که از چند کامپیوتر استفاده می کنند، بسیار کاربردی است و این قابلیت در POP3 وجود ندارد. البته برخی از ISPها به خوبی از IMAP پشتیبانی نمی کنند.

فایل های ضمیمه و تصاویر

در مورد فایل های ضمیمه در ایمیل های دریافتی خود با احتیاط برخورد کنید. در مرحله اول سیستم دانلود خودکار فایل های ضمیمه را در کلاینت ایمیلی خود غیرفعال نمایید. تا حد امکان از دانلود فایل های ضمیمه ای که منتظر دریافت آنها نیستید، خودداری نمایید. حتی اگر دوستان یا همکاران تان در ایمیل شان فایلی را ضمیمه کرده و توضیحی در مورد آن نداده اند، آن را تا حصول اطمینان دانلود نکنید.

همچنین پس از دانلود فایل های ضمیمه شده به ایمیل های دریافتی، آنها را قبل از باز کردن توسط آنتی ویروس اسکن کنید. ضمنا نمایش تصاویری که در متن ایمیل ها وجود دارند را در حالت عادی غیرفعال کنید و ترجیحا اجازه نمایش تصاویری که در متن ایمیل قرار دارند را ندهید. البته برای

مطالعه این درس ها لازم است که این قابلیت فعال باشد تا بتوانید تصاویر درون درس ها را مشاهده کنید.

لینک های درون ایمیل

بسیاری از ایمیل ها حاوی لینک هایی به صفحات خارجی هستند. تا جایی که امکان دارد روی این لینک ها کلیک نکنید. در صورتی که حتما باید این کار را انجام بدهید به جای کلیک کردن، آنها را در نوار آدرس مرورگر کپی و پیست (Paste & Copy) کنید.

اسپم

اسپم ها، ایمیل هایی ناخواسته هستند که اغلب با عناوین و متون تبلیغاتی و اغوا کننده در اینباکس شما ظاهر می شوند. برای اینکه از شر اسپم ها در امان بمانید، لازم است در ابتدا سرویس ایمیلی را انتخاب کنید که قویترین موتور شناسایی اسپم را داشته باشد که جیمیل به عنوان سرویسی رایگان، علاوه بر امنیت بالا، در حال حاضر بهترین مقابله را با ایمیل های اسپم انجام می دهد.

همچنین باید دقت کنید که آدرس ایمیل خود را در هر فرم و لیستی قرار ندهید. همه لیست ها و فرم هایی که ایمیل شما را درخواست می کنند، امنیت لازم را ندارند و ممکن است در واقع اسپمرهایی خودکار باشند. در صورت بی توجهی، ایمیل خود را به اسپمر تحویل داده اید. برای ثبت نام در این فرم ها از ایمیل های موقت استفاده کنید. همچنین می توانید ایمیلی را به همین منظور برای خود ایجاد نمایید و از آن استفاده کنید.

در صورتی که تا حدودی از امنیت ایمیل خود به هنگام ثبت نام به طور کامل مطمئن نیستید، می توانید با مطالعه بخش حریم شخصی یا Privacy Policy از امانت داری سایت مورد نظر مطلع شوید.

آدرس ایمیل تان را جایی یادداشت نکنید

اسپمرها (نرم افزارهایی که به دنبال آدرس های ایمیل می گردند) هر جایی را برای یافتن ایمیل های جدید کاوش می کنند. پس در سایت ها، چت روم ها، لیست های تماس و هر جایی که فکر می کنید ممکن است این یابنده ها در حال جستجو باشند، آدرس ایمیل تان را وارد نکنید. در صورت لزوم ایمیل خود را با فرمت غیر معمول و به طوری که تنها انسانها قادر به شناسایی آن باشند در این مکان ها وارد کنید. برای مثال آدرس myname@gmail.com را به صورت myname[at]gmail[dot]com یا به

صورت «myname در جیمیل» بنویسید. به این صورت تنها افراد قادر به شناسایی ایمیل هستند نه اسپمرها.

همچنین می توانید از سرویس های انکودر استفاده کنید و ایمیل خود را به صورت رمز در بعضی مکان ها وارد و به نمایش افراد بگذارید تا بتوانند در صورت لزوم با شما تماس بگیرند. برای انکود کردن آدرس ایمیل خود می توانید از این سایت استفاده کنید.

نامه های زنجیره ای را فوروارد نکنید

لطفا خرافه پرستی را کنار بگذارید و ایمیل های زنجیره ای را که به طور مثال در آنها نوشته شده است اگر این نامه را برای ۱۰ نفر ارسال کنید حتما تا آخر امروز خبری خوش خواهید شنید، یا آرزویتان برآورده خواهد شد را برای دیگران فوروارد نکنید. کاملا واضح است که این ایمیل ها ارزش فکر کردن هم ندارند چه برسد به ارسال؛ پس امنیت خود را به خطر نیندازید و ایمیل های خود و دوستان تان را به این لیست خوشمزه مورد نظر اسپمرها اضافه نکنید.

در عین حال در صورتی که لازم است ایمیلی را به صورت گروهی به بخش یا تمامی لیست دوستان خود ارسال کنید، لازم است هنگام ارسال، آدرس ایمیل همه‌ی آنها را در بخش BCC وارد کنید. با این کار آدرس های ایمیل پس از ارسال از چشم سایر دوستان و همچنین اسپمرها پنهان می شوند.

ایمیل های اسپم را باز نکنید، پاسخ ندهید و به هیچ وجه فایل های ضمیمه را دانلود نکنید.

همچنین اگر ایمیلی دریافت کردید که مطمئن هستید اسپم است در مرحله اول ترجیحا به هیچ وجه آن را باز نکنید و چنانچه به اشتباه ایمیل را باز کردید، به هیچ وجه به آن پاسخ ندهید. بهتر است با کلیک بر روی کلید Spam آن را به پوشه اسپم انتقال دهید و یا آن را پاک نمایید. در صورتی که اسپمی فایل ضمیمه ای را شامل می شد، تحت هر شرایطی از دانلود آن اجتناب کنید.

ایمیل های جداگانه برای کارهای مختلف در نظر بگیرید

برای اینکه به طور کامل از شر ایمیل های ناخواسته خلاص شوید، استفاده از سه آدرس ایمیل متفاوت توصیه می شود. ایمیل اول برای کارهای شخصی و دریافت و ارسال ایمیل به دوستان و آشنایان در نظر بگیرید. ایمیل دوم به منظور انجام امور شغلی، دریافت و ارسال ایمیل های کاری به

همکاران و سایر شرکت ها ایجاد کنید. در نهایت یک آدرس ایمیل را به منظور ثبت نام در سایت ها و شبکه های اجتماعی که به صورت بالقوه امکان دریافت اسپم از آنها می رود، اختصاص دهید.

می خواهید مرخصی طولانی بروید؟

اگر تصمیم دارید برای مدت زیادی به مرخصی بروید، بهتر است سیستم پاسخ دهی خودکار را فعال کنید تا همه افرادی که برایتان ایمیل می فرستند و منتظر پاسخ هستند را از غیبت تان مطلع کنید. این روش بسیار مودبانه است و فقط یک بار برای ایمیل های مشخص شده ارسال می شود. این کار از دریافت ایمیل هایی که حاوی متن «منتظر پاسخ شما هستم» جلوگیری می کند.

هشدار: هرگز از این سیستم برای ایمیل شخصی خود استفاده نکنید، زیرا چندان جالب نیست دیگران بدانند شما سفر رفته اید و خانه بدون سکنه است.

در صورت رعایت این نکات تا حد زیادی از شر اسپم ها خلاص می شوید.

نکات امنیتی مختص کاربران جیمیل

برای افزایش امنیت حساب جیمیل، انجام این نکات ضروری هستند:

دسترسی سایت ها را به حساب جیمیل تان لغو نمایید: برای انجام این کار در گوگل لاگین کرده و بر روی My Account در گوشه‌ی بالا، سمت راست صفحه‌ی گوگل، کلیک کنید. در صفحه‌ی باز شده، بر روی websites Change authorized کلیک کنید و در صفحه‌ی بعد برای قطع ارتباط سایت های مشخص شده از حساب جیمیل خود، بر روی Revoke Access کلیک نمایید.

امکانات بازیابی اکانت خود را به روز کنید: همانطور که احتمالا می دانید، بازیابی حساب جیمیل، تنها از طریق اطلاعاتی که به عنوان Recovery Options تعریف کرده اید، امکان پذیر است. پس اگر کسی احتمالا از این اطلاعات آگاه شود، این احتمال می رود که موفق به دریافت رمزعبور شما از گوگل شود. برای پیشگیری از این امر، لازم است که این اطلاعات را به روز کنید. البته بسیار مهم است که این اطلاعات را از یاد نبرید.

در جیمیل خود لاگین کرده و به تنظیمات (Settings) آن رجوع کنید. سپس این تغییرات را اعمال یا بررسی کنید:

در تب General، امضا و پاسخ فوری خود را بررسی کنید و در صورت لزوم تغییراتی را برای اختصاصی کردن آنها انجام دهید.

در تب Accounts and Import بررسی کنید که قسمت های Send mail as و Get mail from other accounts و Grant access to your account are all accurate مورد مشکوکی را شامل نشوند. برای مثال دقت کنید که آدرس هایی که در این قسمت ها قابل مشاهده هستند، آشنا بوده و دسترسی های احتمالی برای آنها را خودتان تنظیم کرده باشید، در غیر این صورت این دسترسی ها را لغو کنید.

در تب Filters، فیلترهای موجود را بررسی کنید که ایمیلی به Trash،Spam و یا ایمیل ناشناسی ارسال نشود. در نهایت در تب Forwarding and POP/IMAP مطمئن شوید که ایمیل های شما به آدرس ایمیل ناشناسی ارسال نمی شوند.

در واقع این امکان وجود دارد که ایمیل شما قبلا هک شده باشد و هکر با مراجعه به این بخش ها تنظیماتی انجام داده باشد که همیشه یک نسخه از ایمیل های شما را دریافت کند. دقت کنید بسیاری از هکرها سعی می کنند بی سر و صدا عمل کنند. وقتی ایمیل تان هک می شود قرار نیست شما از چیزی مطلع باشید. هکر دوست دارد شما طبق معمول از صندوق پست الکترونیکی تان استفاده کنید و او هم بدون خبر از مکاتباتتان مطلع باشد. بنابراین مهم است که این بازبینی ها و تغییر رمز عبور را به صورت دوره ای انجام دهید.

در پایین صفحه ایمیل خود، بر روی Details کلیک کنید تا آخرین دسترسی ها به جیمیل خود را مشاهده کنید. در این قسمت IP کامپیوترهایی که از طریق آنها ایمیل خود را چک کرده اید قابل مشاهده است. در صورتی که مورد مشکوکی را مشاهده کردید، لازم است هر چه سریعتر رمز عبور خود را تعویض و نسبت به بررسی مجدد مراحل فوق اقدام کنید.

ایمیل هایی که ظاهرا از طرف گوگل ارسال شده و درخواست ارسال نام کاربری و رمز عبور از شما کرده اند را پاسخ ندهید. گوگل هرگز چنین اطلاعاتی را از شما درخواست نمی کند.

این احتمال وجود دارد که ایمیل هایی حاوی لینک دریافت کنید. در صورتی که بر روی لینک مورد نظر کلیک کردید، به هیچ وجه رمز عبور جیمیل خود را وارد نکنید. حتی اگر ظاهر صفحه شباهت زیادی

به صفحه ورود به جیمیل داشته باشد. برای دسترسی به جیمیل تنها آدرس https://mail.google.com را در مرورگر تایپ کنید.

رمز عبور جیمیل خود را با هیچ سایتی به اشتراک نگذارید. گوگل هیچ سایتی را در مورد عدم سوء استفاده از رمز عبور جیمیل شما، ضمانت نکرده و نمی کند.

اطلاعات مرورگر (Forms, Passwords, Cache, Cookies) را در بازه های زمانی کوتاه پاک کنید. در این مورد در درس امنیت مرورگرها توضیح داده شده است. گزینه Stay signed in را تنها در صورتی تیک بزنید، که از کامپیوتر شخصی خودتان استفاده می کنید.

همیشه پس از اتمام کار با جیمیل، با کلیک بر sign out از آن خارج شوید.

امنیت در چت

امنیت در مسنجرها از مواردی است که باید توجه زیادی به آن داشت. در بسیاری از نرم افزارهای پیام رسان همانند یاهو مسنجر و گوگل تاک که بیشتر از سایر مسنجرها در میان کاربران ایرانی مورد استفاده قرار می گیرند، متن گفتگوی دو نفر به صورت متن ساده، رد و بدل می شود. این مساله یک حفره امنیتی بزرگ برای افرادی است که به هر دلیلی نمی خواهند متن گفتگویشان توسط فرد ثالثی قابل رویت باشد. به این منظور باید از راه هایی برای کد کردن متن چت، استفاده کرد.

توصیه اکید آن است که اگر کاربر جیمیل هستید، از چت جیمیل برای برقراری ارتباط فوری با دوستان و همکاران خود استفاده کنید. چرا که جیمیل به عنوان یک وب میل امن، می تواند تا حد زیادی جلوی بازخوانی متن چت، توسط افراد غیر مجاز را بگیرد.

نرم افزارهای پیام رسان امن

جهت افزایش ضریب امنیتی در چت، استفاده از نرم افزارهای پیام رسان خاصی که قابلیت تجهیز به پلاگین های امنیتی را دارند، توصیه می شود. به این منظور، کاربران ویندوز و لینوکس می توانند از نرم افزار پیجین (Pidgin) استفاده نمایند.

پیجین، نرم افزاری بازمتن و رایگان است که قابل استفاده کاربران مسنجرهای مختلف است. کاربران AIM، IRC، ICQ، Yahoo!، MSN، Google Talk و بسیاری شبکه های دیگر، می توانند به جای

لاگین کردن در تک تک نرم افزارهای پیام رسان خود، به طور همزمان با چندین اکانت در پیجین لاگین کنند.

کاربران مک نیز می توانند نرم افزار آدیوم (Adium) را برای این منظور به کار گیرند، چرا که این نرم افزار نیز همانند پیجین، مسنجرهای مختلف را پشتیبانی می کند.

پلاگین های امنیتی

استفاده از پلاگین های امنیتی جهت حفاظت از متن گفتگو، نکته اصلی این بحث است. OTR یا off-the-record یک پلاگین اختصاصی برای تضمین امنیت چت است. کاربران پیجین باید این پلاگین را دانلود و نصب نمایند.

کاربران آدیوم نیازی به نصب آن ندارند و این پلاگین به صورت پیش فرض بر روی مسنجر آنها نصب است. همچنین کاربرانی که از چت جیمیل برای برقراری ارتباطات فوری استفاده می کنند نیز می توانند از قسمت بالا پنجره چت و در قسمت Actions گزینه Go off the record را انتخاب کنند.

وظیفه OTR

این پلاگین در نرم افزار پیجین اعمال رمزگذاری، شناسایی، کدبندی و امنیت برای کلید امنیتی را داراست. در آدیوم و چت جیمیل نیز عملیات رمز گذاری و غیر قابل ذخیره کردن متن ایمیل توسط این پلاگین انجام می شود. استفاده از OTR مستلزم این است که **نرم افزار پیام رسان دو طرف مجهز به این پلاگین باشد.**

نکاتی در خصوص امنیت در چت

- اطلاعات فردی خود را بروز ندهید. به هنگام ورود اطلاعات در قسمت «نام» در تنظیمات آی دی، اطلاعات فردی و خاص را وارد نکنید. این اطلاعات از نام و نام خانوادگی تا اطلاعات مربوط به تماس و شماره کارت اعتباری شما را شامل می شود.
- با افرادی که در لیست دوستان شما نیستند، به چت و گفتگو نپردازید. در صورتی که کسی را نمی شناسید تا حد امکان از چت کردن با او اجتناب نمایید.

- بر روی لینک های اسپم که در چت باکس نمایان می شوند، کلیک نکنید. شناسایی این لینک ها زیاد سخت نیست. اکثر آنها شامل آدرس های بی معنی و یا تبلیغاتی هستند.

- تا حد امکان از به اشتراک گذاری فایل ها در محیط چت خودداری کنید. این اطلاعات در بسیاری از نرم افزارهای چت به صورت پوینت تو پوینت (P2P) منتقل می شوند و هیچ نظارتی بر آنها وجود ندارد. در این صورت اگر طرف مقابل شما به عمد یا سهوا فایل مخربی را برای شما ارسال کند، ممکن است برای کامپیوتر و حتی اطلاعات شما مضر و خطرناک باشد.

- در صورتی که احساس کردید فردی قصد صدمه زدن به شما را دارد آن را نادیده گرفته یا بلاک کنید. در مواقع لزوم در انجام این کار شک نکنید چرا که ممکن است بعدا به خاطر این شک و تردید، با ضررهای جبران ناپذیری همچون از دست دادن حساب کاربریتان مواجه شوید.

- از نسخه های قدیمی مسنجرها استفاده نکنید. بسیاری از افراد به خاطر قابلیت ها و نرم افزارهای جانبی که بر روی مسنجرشان نصب می کنند از به روز رسانی مسنجرشان طفره می روند، اما باید متذکر شد که این نسخه ها ممکن است حفره های امنیتی ای را شامل شوند که استفاده از آنها می تواند اطلاعات شما را در معرض خطر قرار دهد.

- پلاگین های اضافی را از منابع نامعتبر دانلود نکرده و بر روی مسنجر خود نصب ننمایید.

- پس از اتمام کار با مسنجر حتما Log out یا Sign out نمایید. به یاد داشته باشید که بستن پنجره اصلی مسنجری که استفاده می کنید، عمل خروج را انجام نمی دهد.

- امنیت فیزیکی و شناسایی فرد مقابل در چت: هنگام چت کردن با دوستان و یا همکاران خود، استفاده از پیجین، آدیوم و چت جیمیل، برای امنیت در چت، ضروری است؛ اما باید توجه داشت که آیا فردی در حال نگاه کردن به مانیتور ما یا دوستانمان نیست؟ آیا فردی که با او مشغول گفتگو هستیم واقعا همان دوستمان است؟ این نکات به اندازه رعایت نکات نرم افزاری و امنیت دیجیتال اهمیت دارند. پس لازم است قبل از شروع گفتگو، از این موارد مطمئن شوید. قابلیت شناسایی در پلاگین OTR و در نرم افزار پیجین، در این زمینه به شما

کمک می کند. همچنین می توانید با استفاده از سایر راه های ارتباطی (تلفن و موبایل)، از این مساله مطمئن شوید.

درس چهارم – امنیت در کامپیوترهای عمومی و سفر

حالا وقت اش است سراغ زمانی برویم که در خانه نیستید. در این وضعیت دو حالت متفاوت وجود دارد؛ حالت اول وقتی است که شما با لپ تاپ شخصی تان بیرون می روید و مشغول استفاده از آن در مکان هایی به جز خانه هستید. مثلا در یک کافی شاپ به اینترنت عمومی متصل شده اید و مشغول وبگردی هستید. در این وضعیت شما از کامپیوتر شخصی خودتان استفاده می کنید اما به یک شبکه عمومی متصل هستید. در این حالت باید نکات مهمی برای حفظ امنیت رعایت کنید و ضمنا مراقبت امنیت سخت افزاری لپ تاپ تان هم باشید.

در حالت دوم ممکن است بخواهید از یک کامپیوتر دیگر استفاده کنید. مثلا در یک کافی نت هستید یا در کتابخانه دانشگاه و مدرسه از کامپیوتر عمومی استفاده می کنید یا به خانه دوستتان رفته اید و مشغول استفاده از کامپیوترش هستید.

توجه کنید هر کامپیوتری که مال شخص خودتان نباشد و کس دیگری هم به آن دسترسی دارد را کامپیوتر عمومی تلقی می کنیم. بنابراین حتی اگر از کامپیوتر خواهرتان هم در خانه استفاده می کنید باید آن را یک سیستم ناشناس و خطرناک تلقی کنید.

عجله نکنید! در مورد همه این موارد به کمک این درس، نکات مفیدی خواهید آموخت.

حالت اول: وقتی با لپ تاپ/ موبایل خودم از اینترنت در اماکن عمومی استفاده می کنم.

در این حالت نسبت به وضعیت دوم کمی امنیت بیشتری دارید. اما دقت کنید که گفتیم فقط کمی! اتفاقا وقتی از لپ تاپ شخصی استفاده می کنیم احساس امنیت کاذبی داریم که گاهی اوقات به ضررمان تمام می شود. وقتی به اینترنت یا یک شبکه محلی متصل هستید اطلاعات از لپ تاپ خارج شده و در مسیر تا رسیدن به مقصد از کامپیوترهای مختلفی عبور می کند. فرقی نمی کند از طریق سیم به اینترنت متصل بشوید یا بی سیم. در هر دو صورت این ریسک وجود دارد که اطلاعات ارسالی و دریافتی در راه توسط افرادی به سرقت برود. تصور کنید که رمزهای عبور شما و متن هایی که می نویسد توسط فرد دیگری در راه خوانده شود. هر چقدر هم که لپ تاپ شما امن باشد در مسیر نمی توانید اطمینان داشته باشید که امنیت اطلاعات منتقل شده تامین است یا نه.

امنیت در مسیر انتقال اطلاعات

اطلاعات از لپ تاپ تا رسیدن به مقصد به دو صورت منتقل می شوند:

- متن ساده
- رمزنگاری شده

وقتی اطلاعات به صورت متنی منتقل می شوند، هر کسی که در مسیر آنها را بخواند می تواند از محتوای آنها اطلاع پیدا کند و این اطلاعات شامل آی پی شما هم می شود. بنابراین باید توجه کنید که چه چیزی را دریافت و ارسال می کنید. وقتی از حالت رمزنگاری استفاده می کنید اطلاعات در مسیر قابل خواندن نیست. البته تصور نکنید که به هیچ عنوان قابل خواندن نیستند؛ بسته به قدرت و روش رمزنگاری که استفاده می شود می توان بر روی امنیت ارتباط حساب کرد.

خواندن اطلاعات در شبکه های بی سیم کار آسانی است. هر کسی می تواند در یک شبکه اینترنت بی سیم عمومی با یک نرم افزار، اطلاعات رد و بدل شده توسط دیگران را دریافت و ذخیره کند! بنابراین ممکن است کسی که در کافی شاپ پشت میز آن طرفی با لپ تاپش نشسته، مشغول ذخیره کردن اطلاعات شما باشد.

هنگام استفاده از اینترنت اطلاعاتی که به صورت آدرس HTTPS و رمزنگاری SSL منتقل می شوند در مسیر قابل خواندن نیستند. در آدرس سایت ها به S آخر در HTTPS توجه کنید. وجود آن نشانگر استفاده از رمزنگاری در انتقال اطلاعات است. در این مورد در یکی از درس های این دوره بیشتر صحبت شده است.

سایت هایی که اطلاعات مهمی را رد و بدل می کنند، معمولا از این روش برای انتقال اطلاعات استفاده می کنند. برای مثال وقتی وارد اکانت جیمیل می شوید، می بینید که فرم ورود و صفحات ایمیل با آدرس https آغاز شده اند. اما یاهو فقط برای فرم ورود به ایمیل از این روش استفاده می کند و بعد از ورود به ایمیل بقیه صفحات به صورت متن ساده منتقل می شوند. بنابراین یک هکر در شبکه عمومی رمز عبور یاهوی شما را نمی بیند. اما ایمیل هایی که باز می کنید برایش قابل مشاهده است.

بسیاری از سایت ها حتی هنگام ورود از این روش استفاده نمی کنند. بنابراین وقتی به یک شبکه بی سیم عمومی متصل هستید و وارد اکانت تان در یک فروم می شوید باید روی این ریسک حساب کنید که یک نفر نام کاربری و رمز عبورتان را سرقت کند.

راه حل این است که از ورود به اکانت هایی که از روش امن برای لاگین استفاده نمی کنند خودداری کنید. هر چند راه دیگری هم وجود دارد. در صورتی که یک اکانت VPN داشته باشید که سیستم رمزنگاری مناسبی داشته باشد می توانید با خیال راحت تری از این اینترنت استفاده کنید. VPN یک تونل رمزنگاری شده بین شما و کامپیوتر سرور خودش ایجاد می کند و تمام اطلاعات رد و بدل شده در مسیر به صورت رمزنگاری منتقل می شوند. البته همانطور که گفتیم صرف داشتن یک VPN به معنای امنیت اطلاعات منتقله نیست و باید پروتکل رمزنگاری محکمی برای این ارتباط تعیین شده باشد.

فایروال، فایروال، فایروال

در این دوره با دیوار آتش آشنا می شوید. اما اهمیت داشتن یک فایروال روشن و فعال هنگامی که در یک شبکه عمومی هستید چند برابر می شود. حتما بررسی کنید که در چنین حالتی فایروال لپ تاپ روشن و فعال باشد. این احتمال وجود دارد که به هر دلیلی قبلا آن را غیرفعال کرده باشید و حالا آن را فراموش کرده باشید. چک کردن روشن بودن آن ضرری ندارد.

به اشتراک گذاری فایل و پرینتر را غیرفعال کنید

ممکن است در شبکه خانگی یا محل کار از امکان به اشتراک گذاری فایل و پرینتر استفاده کنید. اما روشن بودن این امکان وقتی به یک شبکه ناشناس متصل هستید به معنی این است که اطلاعات مهم خودتان را دو دستی به دیگران تقدیم کرده اید. این مهم ترین موردی است که کاربران معمولی آن را فراموش می کنند و بعدها افسوس اش را می خورند.

برای خاموش کردن اش در ویندوز اکس پی به بخش My Computer بروید. از منوی Tools در نوار بالا قست Folder Options را انتخاب کنید. یک پنجره جدید باز خواهد شد. حالا بر روی برگه‌ی View کلیک کنید و در لیست پایین گزینه Use Simple File Sharing را غیرفعال کنید. تمام شد! دوباره برای فعال کردن امکان به اشتراک گذاری فایل ها می توانید همین مسیر را بروید و گزینه را فعال کنید.

به روز بودن سیستم عامل

این هم از مواردی است که در درس امنیت سیستم عامل به آن پرداخته شده است. اینجا فقط تاکید می کنیم که به روز نبودن سیستم عامل با آخرین آپدیت ها به معنی ریسک بالای آلودگی با بدافزارها است و معمولا در شبکه های عمومی خیلی بیشتر از شبکه خانگی بدافزار پیدا می شود.

فعال کردن امکان خصوصی سازی فایل ها در ویندوز

سیستم عامل ویندوز امکانی دارد که آن را Private Folder می نامد. با فعال کردن آن، امکان دسترسی هکرها به فایل هایتان کمتر می شود. برای فعال کردن اش در ویندوز اکس پی به درایوی بروید که سیستم عامل ویندوز روی آن نصب شده است که معمولا درایو C است.

وارد پوشه Documents and Settings بشوید و بر روی پوشه ای که هم اسم نام کاربری شما است دوبار کلیک کنید. حالا روی هر پوشه ای که می خواهید راست کلیک کنید و گزینه Properties را انتخاب کنید. در برگه Sharing گزینه Make This Folder Private so that only I have access to it را فعال کنید و تنظیمات را ذخیره کنید.

مراقب اینترنت های مجانی باشید

در کافی شاپ ها یا فرودگاه اغلب اینترنت بی سیم رایگان وجود دارد، اما وقتی به دنبال اینترنت مجانی می گردید احتمالا چندین گزینه برای اینترنت مجانی پیدا می کنید. به این نکته توجه کنید که یک هکر ممکن است با لپ تاپ اش یک شبکه بی سیم با نام مشابه اینترنت مجانی فرودگاه ایجاد کند تا شما به اشتباه به کامپیوتر او متصل شوید! چیزی که اسمش را ظرف عسل می گذارند تا به دام بیافتید.

تصور کنید در فرودگاه هستید و دو شبکه بی سیم با اسم تقریبا مشابه پیدا می کنید. هر دو به نظر می رسد که اینترنت رایگان فرودگاه هستند. اما در واقع یکی از آنها یک شبکه جعلی است که توسط لپ تاپ یک هکر برپا شده تا شما را فریب بدهد. قبلا از متصل شدن به یک شبکه بی سیم مراقب باشید که از حول حلیم در دیگ نیافتید.

حالت دوم: امنیت در کامپیوترهای عمومی

وقتی لپ تاپ ندارید باید با دست خالی به جنگ بروید. اما نه شما آنقدرها هم بی دفاع نیستید. این ها ابزارهای شما در این وضعیت هستند:

حافظه فلش/ فلش مموری

یکی از چیزهایی که همیشه باید همراهتان باشد فلش مموری است. آن هم نه یکی بلکه دو تا! برای اینکه اگر اولی را گم کردید از دومی به عنوان پشتیبان استفاده کنید. در سفر می توانید یکی را به گردن بیاندازید و دومی را در یک جای امن نگه دارید. همان جایی که پول ها را مخفی می کنید! یک کپی کامل از اطلاعات اولی باید روی فلش مموری پشتیبان وجود داشته باشد.

اما اگر فلش مموری به سرقت رفت چه کنیم؟ آن گاه اطلاعات با ارزش ما از دست می رود. به همین خاطر هیچ گاه نباید اطلاعات مهم را بدون رمزنگاری مناسب روی فلش نگه داری کنید. انواعی از فلش مموری ها در بازار فروخته می شوند که اطلاعات را به صورت رمزنگاری روی خودشان نگه داری می کنند و برای دسترسی به اطلاعات روی آنها نیاز به وارد کردن پسورد است. اگر یکی از آنها را داشته باشید، خیالتان در صورت گم شدن فلش تا حد زیادی راحت خواهد بود. اما اگر یک فلش معمولی هم دارید، می توانید با استفاده از نرم افزار true crypt که در این دوره هم با آن آشنا می شوید اطلاعات روی فلش را رمزنگاری کنید. البته برای استفاده از این نرم افزار روی یک کامپیوتر دیگر نیاز است که دسترسی Admin به سیستم عامل داشته باشید، بنابراین همیشه نمی توانید از آن استفاده کنید و بهترین حالت داشتن یک فلش مموری است که خودش امکان رمزنگاری را دارد.

نرم افزارهای پرتابل

تعدادی از نرم افزارهای کاربردی و پر استفاده دارای نسخه به خصوصی هستند که برای استفاده از آن ها نیازی به نصب نرم افزار بر روی سیستم عامل نیست. عدم نیاز این برنامه ها به نصب، باعث می شود که این گونه نرم افزارها را بتوان روی حافظه فلش قرار داد و همراه خود این طرف و آن طرف برد. به همین دلیل نام آن ها را نرم افزارهای پرتابل (قابل حمل) گذاشته اند. فقط لازم است که پوشه نرم افزار پرتابل را روی حافظه فلش قرار دهید. بعد از آن، بر روی تمام کامپیوترهایی که از سیستم عامل مشابهی استفاده می کنند می توانید از روی حافظه فلش و بدون نیاز به نصب، نرم

افزار را اجرا و از آن استفاده کنید. استفاده از نرم افزارهای پرتابل مانند مرورگر پرتابل سبب می شود که ردپای سایت های بازدید شده، بر روی «حافظه فلش» ثبت شود. با بردن حافظه فلش، رد پای خود را هم به همراه خواهید برد. حتی اگر جزو کسانی هستید که لپ تاپ خود را همه جا به همراه می برید، با مواردی رو به رو می شوید که امکان استفاده از لپ تاپ برای اتصال به اینترنت را ندارید و تنها راه نجات شما برای استفاده امن از اینترنت، نرم افزارهای پرتابل است. بنابراین باید همیشه یک مجموعه خوب و بدرد بخور از نرم افزارهای پرتابل را همراه و بر روی فلش مموری خود داشته باشید.

تهیه آن هم کار آسانی است. سایت Portable Apps.com مجموعه کامل و رایگانی از نرم افزارهای پرتابل را در اختیار شما قرار می دهد. کافی است یکی از بسته هایش را دانلود کنید تا بیشتر نرم افزارهای پرتابل مورد نیاز را یکجا بر روی فلش مموری خود داشته باشید.

نرم افزار مدیریت رمزهای عبور پرتابل

در این دوره در درسی مجزا با این نرم افزارها آشنا می شوید. داشتن یکی از این نرم افزارها هنگام سفر یکی از مهم ترین موارد محسوب می شود. نسخه پرتابل Keepass می تواند علاوه بر رمزهای عبور حاوی اسکن اطلاعات مهم مانند کپی شناسنامه، پاسپورت، اطلاعات پزشکی و گواهینامه شما باشد تا در صورت نیاز بتوانید حداقل یک نسخه دیجیتالی امن از آنها به همراه داشته باشید. اگر هم از LastPass استفاده می کنید، می توانید آن را بر روی فایرفاکس پرتابل فلش مموری نصب کنید. برتری Keepass در امکان نگه داری فایل ها به صورت رمزنگاری شده است. کاری که TrueCrypt هم برایتان انجام می دهد، اما برای دسترسی به اطلاعات بر روی KeePass دیگر نیاز به دسترسی Admin نیست، بنابراین همه جا قابل استفاده است.

کی پس پرتابل را دانلود کنید...

چت و تلفن امن

نسخه پرتابل اسکایپ یکی از روش های مناسب برای چت و تماس صوتی به صورت امن محسوب می شود. اسکایپ اطلاعات را به صورت رمزنگاری منتقل می کند، بنابراین خیالتان در این مورد راحت خواهد بود. البته فراموش نکنید که حتی بر روی نسخه‌ی پرتابل اسکایپ هم گزینه‌ی به یاد

داشتن رمز عبور و نام کاربری را فعال نکنید. ضمنا در بخش History نگه داشتن متن چت ها و سابقه تماس ها را غیر فعال کنید. اسکایپ و نسخه پرتابل اش را فقط از مکان های معتبر دانلود کنید، چرا که نسخه های جعلی از آن وجود دارد که برای جاسوسی کردن تماس ها ساخته شده! می توانید اسکایپ پرتابل را از اینجا دانلود کنید.

مخفی کردن هویت

در صورتی که بخواهید هویت خودتان را در یک کامپیوتر عمومی مخفی کنید می توانید از نسخه پرتابل نرم افزار Tor استفاده کنید. این نرم افزار با تغییر آی پی شما سبب مخفی شدن هویت می شود و در واقع یک نرم افزار برای حفظ حریم خصوصی است. البته فراموش نکنید که این نرم افزار اطلاعات منتقل شده را در مسیر رمزنگاری نمی کند و فقط کار تغییر آی پی را برای شما انجام می دهد.

سی دی Live لینوکس

گاهی اوقات این امکان را دارید که از سیستم عاملی که روی کامپیوتر کافی نت نصب شده استفاده نکنید و به جای آن سیستم عامل امن خودتان را داشته باشید. ممکن است ویندوز نصب شده بر روی کامپیوتر کافی نت به انواع جاسوس افزارها و دیگر نرم افزارهای مخرب آلوده باشد. اگر همیشه یک دیسک زنده لینوکس به همراه داشته باشید خیالتان راحت تر خواهد بود. دیسک زنده در واقع یک سیستم عامل کوچک است که از روی یک سی دی یا دی وی دی اجرا می شود. می توانید همیشه یک نسخه از Xubuntu Live CD را به همراه داشته باشید. این یک نسخه عالی و ساده لینوکس است که کار کردن با آن بسیار راحت است. کافی است آن را درون سی دی درایو قرار بدهید و کامپیوتر را ریستارت کنید، آن وقت کامپیوتر بر روی سیستم عامل شما بوت شده و می توانید با خیال راحت کارهای خودتان را انجام بدهید. البته ممکن است روی کامپیوتر کافی نت امکان بوت شدن از روی درایوهای دیگر را غیرفعال کرده باشند، اما اگر این گزینه را داشتید یکی از بهترین کارهایی است که می توانید انجام بدهید. اگر تا به حال با لینوکس کار نکرده اید از امتحان آن نترسید، نیاز نیست که یک خوره کامپیوتر باشید؛ با دو یا سه بار کار کردن می بینید که چقدر آسان است.

رعایت کردن تمام این موارد هنگام کار کردن با کامپیوترهای عمومی امنیت شما را تا حد زیادی بالا می برد. اما باز هم صد در صد خیالتان راحت نباشد! نرم افزارها و حتی سخت افزارهای Keylogger بسیار خطرناکی وجود دارند که اجتناب از آنها بسیار مشکل است، بنابراین وقتی از یک کامپیوتر عمومی استفاده می کنید با وجود تمام این مراقبت ها سراغ انجام هر کاری نروید و بهتر است از وارد شدن به اکانت های بسیار حساس خود مانند حساب های بانکی و... خودداری کنید.

نکات امنیتی سخت افزاری در سفر

تا اینجا در مورد امنیت نرم افزاری در سفر صحبت کردیم، اما بقیه داستان شامل امنیت سخت افزاری می شود. پس این نکات مهم را هم از دست ندهید:

- اگر از لپ تاپ استفاده می کنید آن را همیشه به همراه داشته باشید. حتی اگر فکر می کنید که چند لحظه دیگر بر می گردید هرگز لپ تاپ را تنها جایی رها نکنید. رها کردن لپ تاپ در مکان های عمومی مانند کتابخانه و کافی شاپ ها یک دعوت برای دسترسی به اطلاعات یا نصب نرم افزارهای جاسوسی است.
- وقتی به لپ تاپ تان نیاز ندارید، خاموش اش کنید. در این صورت هم احتمال نفوذ به آن کمتر خواهد بود و هم باتری آن دیرتر تمام می شود.
- از کیف های لپ تاپ تابلو استفاده نکنید. بعضی کیف های لپ تاپ به شدت نشان می دهند که آهای مردم درون این کیف یک لپ تاپ است! بیایید مرا بدزدید! این کیف ها می تواند هدف مناسبی برای سارقان باشد. به جای آن می توانید از یک کیف متفاوت یا یک کوله پشتی استفاده کنید.
- کامپیوتر را بر روی پای خودتان قرار بدهید نه کنارتان یا بالای سرتان. سارقین به راحتی آن را از کنارتان بلند می کنند بدون اینکه متوجه شوید. ممکن است فردی دیگر کیف را اشتباهی بردارد. به خصوص در هنگام شلوغی، استرس و فشار جمعیت.

- لپ تاپ را درون چمدان با بقیه بار و وسایل قرار ندهید. ممکن است در حمل و نقل آن توجه کافی به کار برده نشود و به کامپیوتر شما آسیب برسد. اگر مجبور به این کار هستید آن را در کیسه های حباب دار محافظ بپیچید.
- هنگام سفر لپ تاپ را به طور کامل خاموش کنید و آن را بر روی حالت Stand By یا Hibernate قرار ندهید.
- از رمزهای عبورتان محافظت کنید. آنها را جایی ننویسید. دقت کنید هنگام تایپ ممکن است کسی از روی دست شما نگاه کند؛ این یکی از معمول ترین روش ها برای سرقت رمز عبور است! هیچ رمز عبوری را درون کیف لپ تاپ قرار ندهید.
- شما باید قبل از سفر به فکر این باشید که اگر بلایی سر کامپیوترتان آمد از قبل پیش بینی های لازم را انجام داده باشید. از اطلاعات خود پشتیبان بگیرید. اغلب افراد حال و حوصله پشتیبان گیری از اطلاعات را ندارند. اما سفر یک ریسک بزرگ است، بنابراین قبل از سفر وقت بگذارید و از اطلاعات تان پشتیبان گیری کنید. پشتیبان ها را به همراه نبرید. همیشه به این فکر کنید که ممکن است اطلاعات مهم را در سفر بر اثر یک حادثه از دست بدهید.
- نام، مدل و شماره سریال لپ تاپ تان را یادداشت کنید و در جای امنی نگه داری کنید تا اگر لپ تاپ شما به سرقت رفت و پیدا شد براساس آن بتوانید کامپیوتر خودتان را شناسایی کنید.
- سارقان معمولا سعی می کنند که شکل ظاهری لپ تاپ ها را تغییر دهند تا قابل شناسایی نباشند. اگر بر روی کامپیوترتان علامت شناسایی ویژه ای تعبیه کنید که فقط خودتان از آن مطلع باشید از طریق آن می توانید لپ تاپ کشف شده را شناسایی کنید. همانطور که لپ تاپ ها زیادتر شده اند، آمار سرقت آنها نیز بیشتر شده است. مراقب باشید که کامپیوتر و از آن مهم تر اطلاعات خودتان را به خاطر سهل انگاری از دست ندهید. فراموش نکنید ۹۷ درصد لپ تاپ های سرقت شده هیچ وقت پیدا نمی شوند، بنابراین اگر لپ تاپ تان را از دست بدهید احتمالا باید با آن خداحافظی کنید. همیشه به منطق خودتان احترام بگذارید، وضعیت را تحلیل کنید و براساس آن تصمیم درست را بگیرد.

درس پنجم – آشنایی با مهمترین تهدیدهای امنیتی

پیش از هر کاری لازم است اطمینان یابید کامپیوترتان در برابر هکرها (Hackers) آسیب پذیر نیست و یا توسط نرم افزارهای مخرب (مانند ویروس ها یا برنامه های جاسوسی) که به مالور (Malware) مشهورند، تصرف نشده است. در غیر این صورت، درباره میزان تاثیر اقدامات پیشگیرانه نمی توان هیچ گونه تضمینی داد. خلاصه اینکه، وقتی آقای دزد در زیرزمین خانه مخفی شده، قفل کردن در خانه چندان فایده ای ندارد. بسیاری از کاربران تصور می کنند که همه خطرات در ویروس ها خلاصه شده است، اما ویروس ها فقط بخشی از دنیای بدافزارها را تشکیل می دهند. در این درس به معرفی مالورها می پردازیم، چرا که تا وقتی خطرات را نشناسید، نمی توانید به مقابله با آنها بروید.

مالور یا بدافزار

واژه مالور کوتاه شده ی نرم افزار مخرب (Malicious Software) است. این واژه اصطلاحی عمومی برای توصیف تمام ویروس ها، کرم ها، اسپای‌ورها (Spyware)، ادورها (Adware)، تروجان ها و ... و تقریبا هر چیزی که به طور خاص برای صدمه به کامپیوتر و یا سرقت اطلاعات طراحی شده، می باشد. در این درس با هر کدام از آنها و توانایی هایشان به صورت مختصر آشنا می شوید.

آسیب های مالورها

اکثر مالورها از کامپیوترها به عنوان محلی برای عبور استفاده می کنند. آنها معمولا بدون اینکه آسیبی برسانند از کامپیوتری به کامپیوتر دیگر منتقل می شوند. اما یک مالور خطرناک می تواند به اطلاعات کامپیوتر شما آسیب برساند. این موضوع شامل اطلاعات کول دیسک و هاردهای اکسترنال نیز می شود. همچنین مالورها می توانند کنترل کامپیوتر شما را در دست گرفته و از آن برای حمله به دیگر افراد استفاده کنند. خوشبختانه ابزارهای آنتی مالور (Anti Malware) زیادی برای حفاظت از شما و افراد مرتبط با شما وجود دارد. در زیر به انواع مالورها می پردازیم.

ویروس ها گویی با خراب کردن فایل ها، می خواهند انتقام بگیرند

واژه ویروس های کامپیوتری اغلب به جای مالور استفاده می شود، هر چند در واقع این دو واژه به یک معنی نیستند. در دقیق ترین معنی، ویروس برنامه ای است که مدام تکثیر شده و کامپیوتر را با گسترش خود از یک فایل به فایل دیگر آلوده می کند؛ سپس وقتی فایل ها از یک کامپیوتر به دیگری

کپی شده و بین دو یا چند کامپیوتر به اشتراک گذاشته می شوند، از کامپیوتر آلوده به دیگران منتقل می شود و این روند همچنان ادامه پیدا می کند.

اکثر ویروس ها خود را به فایل های اجرایی متصل می کنند، اما برخی می توانند به فایل های ذخیره اطلاعات بوت، اسکریپت فایل های اتوران (autorun)، فایل های آفیس و... متصل شوند. بسیاری از ویروس ها برای کند کردن و در نهایت غیر قابل استفاده شدن کامپیوتر طراحی شده اند. آنها به سادگی فایل های شما را خراب می کنند. نقطه نظر کلی این است: «ویروس ها برای خراب کردن و از بین بردن اطلاعات طراحی شده اند».

شما می توانید با استفاده از نرم افزارهای آنتی ویروس که همیشه آخرین آپدیت (Update) آنها را انجام داده اید و اجتناب از باز کردن فایل های مشکوک در ایمیل و مکان های دیگر، تا حد زیادی از حملات ویروس ها در امان بمانید. سعی کنید به پسوند فایل ها توجه ویژه ای داشته باشید. مثلا اگر فایلی قرار است mp3 باشد و پسوند آن به شکل mp3.exe است، به احتمال بسیار زیاد شما با یک ویروس سروکار دارید! در این درس قرار است ابتدا با مهمترین تهدیدها آشنا شوید. در درس های بعدی با ابزارهای مناسب برای حذف آنها آشنا می شوید.

کرم ها از طریق شبکه، سیستم ها را آلوده می سازند

کرم های کامپیوتری (Computer Worms) گروهی از مالورها هستند که از شبکه برای ارسال نسخه های خود به کامپیوترهای شخصی دیگر استفاده می کنند. معمولا این کار با استفاده از یک حفره امنیتی برای انتقال از یک کامپیوتر به کامپیوتر دیگر انجام می گردد، که اغلب به طور خودکار و بدون دخالت کاربر اتفاق می افتد. از آنجا که کرم ها معمولا از شبکه ها برای گسترش استفاده می کنند و هر کامپیوتری را در مسیر خود آلوده می کنند، از آنها به عنوان شایع ترین نوع مالورها یاد می شود. اگر چه هنوز بسیاری از کاربران به اشتباه از آنها به عنوان ویروس یاد می کنند.

نکته: به مالوری که تحت شبکه کار کند، Botnet یا ربات شبکه نیز می گویند.

کرم ها با ویروس ها تفاوت دارند. ویروس ها با اتصال به برنامه های دیگر منتقل و تکثیر می شوند. به عبارت دیگر تا زمانی که با کامپیوتر آلوده به ویروس کار نکنید، ویروس گسترش بیشتر نخواهد

یافت. اما کرم ها بی نیاز از برنامه های دیگر می توانند خودشان را به طور مرتب در کامپیوتر میزبان یا دیگر کامپیوترهای مرتبط کپی کنند و جابجا شوند.

یکی از معروف ترین کرم ها عبارت است از کرم ILOVEYOU که به صورت ضمیمه ایمیل منتقل می شد. این کرم به شرکت های تجاری بیش از ۵/۵ میلیارد دلار خسارت وارد کرد. Code Red کرم معروف دیگری است که ۳۵۹۰۰۰ وب سایت را آلوده کرد و برای یک دوره کوتاه، سرعت جهانی اینترنت را کم کرد! مورد معروف بعد Blaster نام داشت، این کرم باعث راه اندازی مجدد کامپیوتر به طور مکرر می شد

از آنجا که کرم ها معمولا از آسیب پذیری شبکه سوء استفاده می کنند، راه جلوگیری از حملات شان فعال و قفل کردن فایروال است. البته در مورد کرم هایی که قبلا وارد سیستم شده اند، نیاز به یک آنتی ویروس نیز خواهید داشت.

اسب های تروجان، یک در پشتی درون سیستم شما

اسب های تروجان (Trojan Horses) برنامه هایی هستند که در ظاهر در حال انجام کار بی ضرری هستند، اما در خفا دارای کدهای مخربی اند که کار دیگری انجام می دهند. در بسیاری از موارد، تروجان ها یک در پشتی (Back Door) روی کامپیوتر طعمه قرار می دهند که اجازه کنترل از راه دور کامپیوتر آلوده را به سازنده شان می دهد. یک کامپیوتر آلوده معمولا به صورت مستقیم یا به عنوان عضوی از شبکه آلوده مورد سوء استفاده قرار می گیرد. تفاوت عمده بین ویروس و کرم با تروجان این است که تروجان خود را تکثیر نمی کند. همچنین تروجان توسط کاربر به شکل ناآگاه نصب می شود.

نکته: در پشتی به یک نقص در سیستم عامل یا نرم افزارهایش گفته می شود که حکم یک راه ورودی مخفی برای هکر را دارد.

هنگامی که کامپیوتر شما به تروجان آلوده شد، طراح تروجان می تواند از آن برای هر هدف بدی استفاده کند، مانند حملات (DoS=Denial of Service) به یک وب سایت، استفاده از پراکسی سرور برای مخفی کردن حملات و یا حتی بدتر، برای ارسال ده ها اسپم (هرزنامه). حفاظت در مقابل حملات تروجان ها، همانند روش حفاظت در مقابل ویروس ها است:

- مطمئن شوید، برنامه آنتی ویروس شما به روز (آپدیت) شده است.
- هیچ گاه فایل پیوست (Attachment) مشکوک در ایمیل را باز نکنید.
- قبل از اینکه فایل های کرک را برای برنامه ای مثل فتوشاپ دانلود و نصب کنید، به عواقب احتمالی اش خوب فکر کنید. چون اصولا فایل های کرک مکانی ایده آل و مورد علاقه تروجان نویسان برای مخفی کردن تروجان است. بنابراین بهترین راه این است که از نرم افزارهای قفل شکسته استفاده نکنید. اغلب اوقات جایگزین های رایگان و مناسبی برای انجام کارها پیدا می شود.

اسپم (Spam)

اسپم به هر پیامی با اهداف بد یا تبلیغاتی گفته می شود که بدون درخواست شما به دستتان رسیده است. نوع ایمیلی آن (Email Spam- هرزنامه) می باشد که به ایمیلی با اهداف بد (حاوی مالور یا تبلیغاتی) گفته می شود.

اسپای ورها، دزد اطلاعات شما هستند

جاسوس افزار (Spyware) عبارت است از هر نرم افزار نصب شده بر روی کامپیوتر، که اطلاعات را بدون اطلاع شما جمع آوری کرده و به سازنده خود بفرستد. سازنده برنامه از اطلاعات شخصی شما، برای مقاصد سوء خود استفاده می کند. ممکن است این جاسوسی به شکل (keylogging یا جاسوسی صفحه کلید) برای کشف و استفاده از پسورد، تماشای نتایج جستجو، تغییر صفحه خانگی و موتور جستجوی مرورگر شما، اضافه کردن نوار ابزار مضر یا ناخواسته به مرورگر و یا سرقت شماره کارت اعتباری شما باشد.

به نرم افزاری که عمل keylogging را انجام دهد، کی‌لاگر (Keylogger) گفته می شود. این نرم افزار تمام کلیدهایی که در صفحه کلید می زنید، به ترتیب ذخیره و برای سازنده خود می فرستد. از آنجا که اسپای ورها عمدتا به منظور کسب درآمد از جیب شما طراحی شده اند، معمولا نیازی به خرابکاری در کامپیوتر ندارند، به همین دلیل بسیاری از کاربران از وجود آنها اطلاع ندارند، فقط ممکن است سرعت سیستم را پایین بیاورند. بنابراین به کاهش سرعت کامپیوترتان حساس باشید.

ادورها، تبلیغات بازرگانی ناخواسته ی دنیای کامپیوتر

تبلیغ افزار (Adware) مالوری است که به نمایش اجباری تبلیغات در کامپیوتر می پردازد. در نگاه اول ممکن است فکر کنید نمایش تبلیغات برای کامپیوترتان ضرری ندارد، اما هیچ تضمینی وجود ندارد که یک ادور علاوه بر نمایش تبلیغ به فعالیت های مخفی و مضر دیگری نیز مشغول نباشد. در ضمن این احتمال وجود دارد، ادور با ورود خود راه را برای دیگر مالورها باز کند، ضمن اینکه آنها پهنای باند اینترنت شما را هم مصرف می کنند.

برای محافظت در برابر اسپای ورها و ادورها نیاز به نصب یک آنتی اسپای ور دارید. متاسفانه اکثر افراد فکر می کنند همه آنتی ویروس ها قابلیت شناسایی اسپای ورها و ادورها را دارند، در حالی که چنین نیست. شما باید از فروشنده بپرسید تا مطمئن شوید آنتی ویروس شما آنتی اسپای ور نیز هست یا خیر؟ در درس آشنایی با نرم افزارهای ضدجاسوس افزار و تبلیغ افزار با این ابزارهای مقابله آشنا می شوید.

روت‌کیت ها در هسته سیستم پنهان می شوند

RootKit همان طور که از نام آن پیداست در هسته (Root) سیستم پنهان می شود. این مالورها ابتدا از نقاط ضعف سیستم استفاده کرده و خود را به هسته سیستم عامل می رسانند، سپس در آنجا پنهان شده و به اهداف مخرب خود می پردازند. حتی ممکن است از درون کد خود، یک مالور (ویروس، کرم یا...) آزاد کنند. برای پاک کردن این مالورها به آنتی ویروس نیاز دارید. معمولا پاک کردن این مالورها مشکل می باشد.

حقه بازی اینترنتی یا Spoofing چیست؟

Spoofing یا حقه بازی اینترنتی عبارت است از اینکه هر شخص، شرکت، وب سایت، و یا سرور ایمیلی، با جعل عنوان یا تغییر هویت، قصد کلاهبرداری، حقه بازی یا حتی تمسخر کاربر را داشته باشد. پرکاربردترین شیوه Spoofing در فضای اینترنت، استفاده از ایمیل و وب سایت است.

کلاهبرداری ایمیلی (Email Spoofing): عبارت است از پنهان کردن آدرس فرستنده به گونه ای که به نظر نیاید ایمیل از طرف یک ناشناس برای شما فرستاده شده است. برای مثال ایمیلی ظاهرا از طرف

سایت یاهو برای شما می آید و از شما خواسته در پاسخ، برای انجام برخی امور، پسورد ایمیل خود را برایشان بفرستید.

کلاهبرداری وب سایتی (Website Spoofing): این روش به Phishing معروف است و یکی از خطرناک ترین روش های کلاهبرداری اینترنتی است. باید مراقب باشید تا گیر این حملات نیافتید. کاربر با مراجعه به یک سایت تقلبی که ظاهری مشابه یک سایت معروف دارد، بدون توجه به آدرس آن و با فرض اینکه این صفحه همان سایت مورد نظرش است، نام کاربری و پسورد خود را می نویسد. با این کار به راحتی نام کاربری و پسوردش را تقدیم کلاهبردار می کند. معمولا فرد کلاهبردار آدرس صفحه را نیز مشابه سایت اصلی انتخاب می کند، تا شما را به اشتباه بیاندازد. برای مثال اگر آدرس ورود به ایمیل یاهو به این شکل باشد:

http://login.yahoo.com

فرد کلاهبردار سعی می کند آدرسی شبیه به آن تهیه کند. برای مثال:

http://login.yahsooo.com

اگر دقیق نباشید ممکن است اطلاعات مهم تان را دو دستی تقدیم کلاهبردار بکنید.

Clickjacking یا کلیک دزدی چیست؟

کلیک جکینگ (کلیک دزدی) یک روش هوشمندانه است برای ترغیب یا مجبور کردن کاربران به کلیک کردن بر روی چیزی، بدون اینکه از محتوای آن آگاه باشند. این تکنیک به شکل های مختلفی اتفاق می افتد و ممکن است هر کاربری را فریب دهد، اما با کمی دقت می توان از آسیب های این روش در امان ماند.

برای مثال شما ایمیلی دریافت می کنید که ظاهرا لینکی به ویدئوی مهمترین خبر روز در آن وجود دارد، اما لینک در واقع صفحه فروش محصولی در سایتی غیر معتبر است. با فشار دادن کلید Play در ایمیل به جای اجرای ویدئو، شما با صفحه فروش محصول مواجه می شوید.

از Clickjacking در موارد زیر هم استفاده می شود:

- اجازه گرفتن از کاربر برای فعال کردن وب‌کم و میکروفون

- ترغیب کاربر به فعال کردن پروفایلش برای بازدید عموم
- فالوشدن در توئیتر
- داغ کردن لینک ها در شبکه های اجتماعی
- و...

راه مقابله

نکته مهمی که در بسیاری موارد به کاربر کمک می کند تا از دزدیده شدن کلیک ها و خطرات احتمالی بعدی در امان بماند، دقت در آدرس هر لینک است. حتما دقت کرده اید، اگر نشانگر موس خود را بر روی یک لینک بیاورید، قبل از اینکه کلیک کنید آدرس لینک در پایین و سمت چپ مرورگر نمایش داده می شود. با تطبیق توضیحات لینک و آدرس مربوطه، می توانید در موارد زیادی تشخیص دهید این لینک معتبر هست یا نه. البته این هم به طور کامل نمی تواند مانع کلیک جکینگ شود، اما دقت در آدرس واقعی لینک ها قبل از کلیک شدیدا توصیه می شود.

حملات اکس اس اس

Cross Site Scriptin یا به صورت خلاصه «اکس اس اس» یکی از رایج ترین حملاتی است که در حال حاضر کاربران وب را هدف گرفته است. در این نوع حمله با باز کردن یک صفحه اینترنتی، کلیک کردن روی یک لینک و یا باز کردن ایمیل، کدی به صورت مخفیانه بر روی کامپیوتر کاربر اجرا می شود که می تواند اطلاعات مهمی را از روی کامپیوتر کاربر سرقت کند.

ماهیت این حمله به گونه ای است که اغلب کاربران تصورش را هم نمی کنند که ممکن است به همین سادگی اطلاعات خودشان را از دست بدهند، به همین دلیل این نوع حمله دست کم گرفته می شود. برای مثال کاربر روی لینکی که توسط ایمیل برای او فرستاده شده کلیک می کند و یک صفحه اینترنتی را باز می کند، با انجام این کار، هکر می تواند کوکی مربوط به ایمیل کاربر را سرقت کند و از طریق آن وارد ایمیل کاربر بشود تا به اطلاعات او دسترسی پیدا کند.

این سناریو در مورد بقیه حساب های کاربری اینترنتی هم امکان پذیر است. در حملات اکس اس اس فقط با مشاهده یک صفحه اینترنتی که کدهای حمله در آن مخفی شده اند، کامپیوتر مورد حمله قرار می گیرد و کاربر هم از آن مطلع نمی شود.

زمانی که کاربر وارد یک حساب اینترنتی مانند ایمیل، حساب بانکی یا حساب های کم اهمیت تر می شود، اطلاعاتی توسط سرورهای این حساب ها روی کامپیوتر استفاده کننده ذخیره می شود. حملات اکس اس اس می توانند این اطلاعات را از روی کامپیوتر کاربر بربایند و هکر با داشتن این اطلاعات به حساب اصلی دسترسی پیدا کند.

به عنوان مثال کاربری در حال خواندن یک صفحه وب است که به کدهای مخرب آلوده است و همزمان در حساب بانکی خود هم وارد شده است. هکر می تواند با مخفی کردن یک کد در صفحه ای که توسط کاربر در حال خوانده شدن است، از ضعف سیستم بانکی استفاده کرده و وارد حساب بانکی او بشود.

یکی از بهترین روش های جلوگیری از این حملات استفاده از افزونه No Script بر روی مرورگر فایرفاکس است که در درس امنیت مرورگر با آن آشنا شدید.

آنتی ویروس های جعلی

در این روش کاربر چیزی را که به نظر یک نرم افزار آنتی ویروس رایگان واقعی می رسد، دانلود می کند. پس از نصب این برنامه و اسکن کامپیوتر، برنامه به شما خواهد گفت که کامپیوترتان آلوده به صدها نوع ویروس است. برنامه هم تنها در صورتی می تواند کامپیوتر شما را تمیز کند که شما برای نسخه کامل برنامه مقداری پول پرداخت کنید. به این مالورها، باج افزار (Scareware) نیز می گویند؛ البته نرم افزارهای Scareware چیزی بیش از یک مالور هستند. باج افزار، کامپیوتر شما را تا زمانی که به طراح برنامه پول پرداخت نکنید به گروگان نگه می دارد. در اکثر موارد، شما نمی توانید آنها را از روی کامپیوتر خود حذف کرده و یا در برخی موارد حتی از کامپیوتر استفاده کنید.

درس ششم – آنتی ویروس ها و انتخاب آنها

تقریبا همه کاربران می دانند که روی سیستم عامل ویندوز نیاز به نصب آنتی ویروس داریم. اما چه آنتی ویروسی؟

نرم افزارهای ضد ویروس زیادی وجود دارند که می توانند کامپیوتر را در برابر ویروس ها حفظ کنند؛ لازم است در انتخاب آنتی ویروس و استفاده از آن، دقت کنیم. چرا که باید آگاه باشیم آنتی ویروسی مناسب است که بتواند علاوه بر حفاظت کامپیوتر در برابر ویروس ها، مصرف حافظه ی کمتر و قابلیت های بیشتری را نیز در اختیار ما قرار بدهد. با توجه به این توصیفات، در ادامه ی این درس به نکاتی در خصوص شناسایی نرم افزارهای ضد ویروس مناسب و قابلیت های مهمی که در اکثر آنها وجود دارد، می پردازیم.

ویروس ها اغلب باعث اختلال در عملکرد کامپیوتر می شوند و برخی نیز با هدف قرار دادن نرم افزارها یا سخت افزارهای خاصی خساراتی را نیز به بار می آورند. البته ویروس تنها یکی از نمونه های بد افزارها است. مالورها (Malwares) انواع مختلفی دارند. ویروس، کرم، تروجان، Backdoor ، Keylogger، Spyware، RootKit، Adware،ScareWare و... تعدادی از شایع ترین بد افزارهای شناخته شده هستند. در درس آشنایی با بدافزارها با انواع آنها به طور کامل تر آشنا شده اید.

خصوصیات یک نرم افزار آنتی ویروس مناسب

شناسایی هوشمندانه ویروس ها

یکی از قابلیت های اساسی یک آنتی ویروس مناسب، شناسایی ویروس ها است. بسیاری از آنتی ویروس ها، کتابخانه ای از اطلاعاتی را در مورد ویروس های مختلف در خود دارند که برای شناسایی و نابودسازی ویروس های فعلی و حتی برخی ویروس های جدید، به نرم افزار آنتی ویروس کمک می کند. یک آنتی ویروس مناسب، مجهز به موتور هوشمند شناسایی و پاک سازی ویروس های جدید است.

به روز رسانی

همه روزه بد افزارهای جدید و جدیدتری ساخته و منتشر می شوند. به روز رسانی آنتی ویروس، برای پیشگیری از بروز مشکلاتی که این بد افزارها می توانند برای ما به وجود آوردند، از اهمیت ویژه ای

برخوردار است. پس از اینکه ویروسی جدید کشف می شود، شرکت های تولید کننده آنتی ویروس ها در سریع ترین زمان ممکن، بسته های امنیتی مربوط به آن را منتشر و در اختیار کاربران قرار می دهند. آنتی ویروسی که مورد استفاده قرار می دهید، باید در فواصل زمانی کوتاه، با بسته های به روز رسانی کم حجم، آپدیت شود و امکان به روز رسانی خودکار نیز در آن وجود داشته باشد.

دانستن این نکته مهم است زیرا اگر شما آنتی ویروس دارید اما آن را به طور مرتب آپدیت نمی کنید، این کار هیچ تفاوتی با نداشتن آنتی ویروس ندارد. بنابراین یک آنتی ویروس که آپدیت نمی شود در عمل بی فایده است.

توجه: علاوه بر آنتی ویروس، به روز رسانی همه ی نرم افزارهای مورد استفاده و همچنین سیستم عامل در حفظ امنیت و حفاظت از داده ها و اطلاعات شما، از اهمیت ویژه ای برخوردار است.

اسکن اطلاعات ذخیره شده در هارد

توانایی پویش و جستجوی سریع همه یا قسمتی از هارد کامپیوتر (فایل ها و پوشه ها) اسکن نامیده می شود. این قابلیت از خصوصیات یک آنتی ویروس مناسب است و فاکتورهای سرعت و دقت را شامل می شود. لازم است که هر از چند گاهی تمامی هارد خود را با گزینه Full Scan که در اکثر آنتی ویروس ها وجود دارد، اسکن کنید. بدین ترتیب فایل های مخرب احتمالی که در پوشه ها و حتی فایل های شما جا خوش کرده اند، شناسایی شوند. اهمیت اسکن در حفظ امنیت و حفاظت از فایل ها و پایداری ویندوز شما، بسیار زیاد است.

صندوقچه ویروس ها یا مکانی برای قرنطینه

در بسیاری از آنتی ویروس های معتبر و کاربردی، امکانی وجود دارد که با استفاده از آن می توان ویروس های شناسایی شده را در مکانی امن قرنطینه کرد. این مکان امن همان Virus Chest یا Quarantine است. تصور کنید که فایل مهمی دارید که با ویروسی ناشناخته آلوده شده است. در صورتی که آنتی ویروس تان فایل مورد نظر را ویروس تلقی کند، هنگام پاکسازی، ممکن است به خاطر ناشناخته بودن ویروسی که فایل شما را آلوده کرده، به جای پاکسازی فایل از ویروس، آن را کاملا پاک نماید. برای جلوگیری از این اتفاق می توانید فایل مورد نظر را در صندوقچه ویروس ها قرنطینه کنید، به این امید که در آپدیت های بعدی، آن را دوباره چک کرده و احتمالا پاکسازی نمایید.

قابلیت های اضافی و نکات ضروری

علاوه بر قابلیت های اشاره شده، لازم است که آنتی ویروس به خصوصیات اضافی ای نیز مجهز باشد.

سپرهای محافظتی که رفتارها و ارتباطات مشکوک را بررسی می کنند و در صورت مشاهده موارد نامتعارف، بسته به تنظیماتی که اعمال می کنید، اخطار داده یا از بروز اشکال جلوگیری می کنند.

آنتی ویروس را به گونه ای تنظیم کنید که دائما در حالت آماده به کار باشد و با بالا آمدن ویندوز فعال شود. این قابلیت در محصولات مختلف نام های متفاوتی دارد. ممکن است با عباراتی شبیه Realtime Protection و یا Resident Protection نامیده شود.

به طور منظم تمامی فایل های کامپیوتر را برای یافتن ویروس ها اسکن (Scan) کنید. نیازی نیست این کار را هر روز انجام دهید، به خصوص اگر Realtime Protection آنتی ویروس تان را فعال کرده باشید. توصیه می شود حداقل هفته ای یک بار کامپیوتر خود را اسکن کنید.

امکان اسکن در حالت بوت از قابلیت های ضروری یک نرم افزار ضد ویروس است. آنتی ویروس ها با استفاده از این قابلیت توانایی شناسایی ویروس های احتمالی را قبل از شروع به کار ویندوز پیدا می کنند.

گزارش گیری در مورد عملکرد نرم افزار، از قابلیت های اضافی و مهم یک آنتی ویروس قدرتمند به حساب می آیند.

میزان مصرف رم و پردازنده

آنتی ویروس به هر شکل مقداری از فضای رم و پردازش CPU را به خود اختصاص می دهد. اما باید دقت داشت که این مقدار نباید از حدی تجاوز کند که در این صورت با افت سرعت کامپیوتر مواجه می شوید.

آنتی ویروس؛ رایگان یا تجاری؟

بسیاری از افراد تصور می کنند، آنتی ویروس های پولی از قدرت و امنیت بیشتری نسبت به آنتی ویروس های رایگان برخوردارند. حتی برخی افراد آنتی ویروس های پولی را با روش های مختلف کرک می کنند، چرا که استفاده از آنها را به استفاده از آنتی ویروس های مجانی ترجیح می دهند. اما باید

توجه داشت، که اکثر آنتی ویروس هایی که به صورت رایگان در اختیار کاربران قرار می گیرند، در جهت شناسایی و نابودسازی ویروس ها در یک کامپیوتر، قدرتی در حد آنتی ویروس های پولی دارند؛ اما تفاوت کجاست؟

اغلب آنتی ویروس هایی که به صورت تجاری به کاربران ارائه می شوند، علاوه بر توانایی در شناسایی ویروس ها و پاک سازی کامپیوتر از آنها، مجهز به موتورها و نرم افزارهای اضافی نیز هستند. برای مثال اسکنرها و سپرهای حفاظتی اضافی مانند Mail Scanner، Web Shield و... ابزارهایی هستند که آنتی ویروس ها و نسخه های اینترنت سکیوریتی از نرم افزارهای حفاظتی شناخته شده، به آنها تجهیز می شوند. این تجهیزات و قابلیت های اضافی، معمولا در آنتی ویروس های رایگان وجود ندارند، اما با نصب نرم افزارهای اضافی در کنار یک آنتی ویروس رایگان، می توان از آنها نیز بهره برد.

نکته مهم: به هیچ عنوان از نسخه های کرک شده آنتی ویروس های پولی استفاده نکنید. این کار علاوه بر کاهش امنیت کامپیوتر شما، منجر به بروز اشکالاتی در توانایی های آنتی ویروس و عدم آپدیت صحیح آن می شود و بدین ترتیب حتی ممکن است سیستمی که به آنتی ویروس مجهز نیست به مراتب از سیستمی که از یک آنتی ویروس کرک شده استفاده می کند، امنیت بیشتری داشته باشد.

همچنین اطمینان یابید، آنتی ویروس به رایگان آپدیت می شود. بسیاری از آنتی ویروس های تجاری یک نسخه نصب اولیه رایگان در اختیارتان می گذارند که برای مدتی کوتاهی می توان از آن استفاده و آن را به روز رسانی کرد؛ اما برای تمدید این زمان نیاز به ثبت نام و پرداخت هزینه دارند. پس از پرداخت هزینه مربوطه، نرم افزار تا پایان مدت زمان مشخص شده، باید کار کند.

به حرف فروشنده ها اعتماد نکنید

اگر قصد خرید آنتی ویروس دارید نمی توانید به حرف فروشنده ها اعتماد کنید. هر کدام از آنها انواع نمودار و بررسی ها به شما نشان می دهند که اثبات می کند آنتی ویروسی که می فروشند بهترین است! در بازار آنتی ویروس از این آمار و ارقام زیاد پیدا می شود، حتی می توانید در سایت های زیادی لیست بهترین آنتی ویروس ها را پیدا کنید. فقط مشکل در اینجاست که لیست هر کدام از سایت ها با دیگری متفاوت است. بنابراین پیش از خرید، خودتان به صورت مستقل تحقیق کنید.

آنتی ویروس های رایگان پیشنهادی

آنتی ویروس ها در مجموع برای محافظت از کامپیوتر شما در برابر ویروس ها، کرم ها و تروجان ها طراحی و ساخته می شوند. البته آنتی ویروس ها بر حسب نوع، ممکن است سایر مالورها را نیز پوشش دهند. برای فهمیدن نوع مالورهای تحت پوشش نرم افزار، می باید اطلاعات مربوط به آن را در سایت رسمی اش بخوانید. اما در ادامه این درس به معرفی چند آنتی ویروس رایگان و معروف که قابلیت های زیادی را در اختیار شما قرار می دهند، می پردازیم و توصیه می کنیم یکی از آنها را انتخاب کنید.

- Avast: یکی از بهترین نرم افزارهای آنتی ویروس موجود برای ویندوز است. کار با این نرم افزار بسیار ساده است، مرتب آپدیت (به روز رسانی) می شود و بسیاری از حرفه ای ها هم از آن استفاده می کنند. دانلود کنید...
- Clam win: یکی از همتاهای اوپن سورس (Open Source) رایگان Avast است که از مشهورترین آنتی ویروس های ویندوزی دنیا به حساب می آید. این نرم افزار یک نسخه پرتابل (قابل جابجایی) دارد که می توان آن را از روی کول دیسک اجرا کرده و کامپیوتری را که اجازه یا امکان نصب برنامه بر روی آن را ندارید، پاک سازی کنید. این قابلیت هنگامی که برای انجام کارهای مهم تان مجبور به استفاده از کامپیوترهای عمومی یا کافی نت ها هستید، بسیار کاربردی است. دانلود کنید...
- Avira: از آنتی ویروس های بسیار خوب و رایگان است که همانند چتری، در برابر باران های اسیدی از کامپیوتر محافظت می کند. دانلود کنید...
- AVG: این آنتی ویروس نیز انتخابی مناسب برای افرادی است که قصد انتخاب یک محافظ مناسب را برای ویندوز خود دارند. دانلود کنید...
- Microsoft Security Essentials: این آنتی ویروس به عنوان ضد ویروس رایگان مایکروسافت انتخاب بسیار خوبی به نظر می رسد. دانلود کنید...

- Sophos - Antivirus for Mac: این آنتی ویروس یکی از آنتی‌ویروس‌های مجانی برای سیستم‌های مک است. می‌توانید از اینجا دانلود کنید.

نکته: هیچ گاه به طور همزمان از دو آنتی ویروس بر روی یک کامپیوتر استفاده نکنید، زیرا این کار می تواند باعث کند شدن شدید و حتی قفل کردن کامپیوتر شود. اگر می خواهید آنتی ویروس جدیدی نصب کنید، حتما قبل از شروع کار آنتی ویروس قبلی را پاک کنید، یک بار کامپیوتر را ریستارت (Restart) کنید و سپس نسبت به نصب آنتی ویروس جدید اقدام کنید.

درس هفتم – نرم افزارهای ضد جاسوس افزار و تبلیغ افزار

در درس آشنایی با تهدیدهای امنیتی با مهم ترین خطرات دنیای کامپیوتر و اینترنت آشنا شدید. حالا نوبت به مقابله با آنهاست، اینجا به طور خاص به نرم افزارهای Anti Spyware می پردازیم. وقتی در مورد نرم افزار آنتی ویروس صحبت می کنیم اغلب منظور نرم افزاری است که ویروس ها و کرم ها را شناسایی و حذف می کند. اغلب کاربران بین تروجان، کرم و ویروس تفاوتی قائل نیستند و همه را به نام ویروس می شناسند. بیشتر نرم افزارهای آنتی ویروس این بد افزارها را شناسایی می کنند، اما وقتی نوبت به جاسوس افزارها و تبلیغ افزارها می رسد ماجرا متفاوت می شود.

همانطور که در درس های قبلی با جاسوس افزارها آشنا شدید، این نرم افزارها کار سرقت اطلاعات شما را انجام می دهند. اغلب اوقات شما از وجود آن ها بر روی کامپیوترتان اطلاع ندارید اما یکی از علامت های وجود چنین بد افزارهایی کُند شدن کامپیوتر است. بنابراین همیشه نسبت به کاهش سرعت کامپیوترتان حساس باشید. شاید یک نرم افزار مشغول جاسوسی کارهای شما یا سرقت اطلاعات تان است.

در حال حاضر آنتی ویروس هایی در بازار موجود هستند که کار تشخیص و حذف جاسوس افزارها و تبلیغ افزارها را هم انجام می دهند، اما همه ی آنها اینگونه عمل نمی کنند. بنابراین در میان کارشناسان امنیتی این نظریه وجود دارد که برای داشتن امنیت بهتر علاوه بر یک آنتی ویروس مناسب شما به یک نرم افزار ضد جاسوس افزار قدرتمند هم نیاز دارید تا پوشش وسیع تری داشته باشید.

در این درس با چند نرم افزار مفید، رایگان و قدرتمند از این دسته آشنا می شوید. می توانید یکی از آنها را انتخاب و بر روی کامپیوتر شخصی تان نصب کنید.

Ad-Aware

این نرم افزار یکی از بهترین انتخاب هایی است که در اختیار دارید. نسخه رایگان آن با قدرت جاسوس افزارها و تبلیغ افزارها را شناسایی می کند و ضمنا حالت بررسی لحظه ای فایل ها را هم دارا می باشد. کار با آن ساده است و در ورژن جدیدش کار شناسایی ویروس ها را هم انجام می دهد. هر چند همچنان کار اصلی اش شناسایی جاسوس افزارها محسوب می شود.

آپدیت آن به صورت خودکار صورت می گیرد و تنها ایراد آن شاید حجم نرم افزار باشد که برای نصب آن مجبور به دانلود بیش از ۱۲۰ مگابایت هستید، اما خواهید دید که ارزش اش را دارد.
دانلود کنید...

Spybot

این هم یکی از نرم افزارهای رایگان و قدرتمند برای مبارزه با جاسوس افزارها است. اگر یک کاربر پیشرفته باشید این یکی از گزینه های خوب شما است، چرا که امکانات فنی زیادی در مقابله با نرم افزار قبلی در اختیارتان قرار می دهد. حجم اش کمتر از ۱۶ مگابایت است. یکی از ایراداتی که به این نرم افزار وارد است، درست کار نکردن آن در بعضی اوقات است که ممکن است با قفل کردن نرم افزار مواجه شوید.
دانلود کنید...

SuperAntispyware (نسخه پرتابل)

این یکی از قوی ترین نرم افزارهای ضد جاسوس افزار به حساب می آید و در کنار آن یک نسخه پرتابل هم از این نرم افزار ارایه شده است که آن را به بهترین انتخاب برای پاک کردن کامپیوترهای دیگران و کامپیوترهایی که از قبل آلوده شده اند تبدیل می کند. مزیت نسخه پرتابل در این است که می توانید آن را بدون نیاز به نصب بر روی حافظه ی فلش خود همیشه همراه داشته باشید و با آن کامپیوترهای آلوده دیگران را هم اسکن و پاکسازی کنید.

سایت این نرم افزار، به ازای هر بار دانلود این نرم افزار، فایل دریافتی را با نام جدیدی در اختیار شما می گذارد، زیرا بسیاری از بد افزارهای قوی از فعال شدن و نصب برنامه های شناخته شده ای که توانایی نابود ساختن آن ها را دارند، جلوگیری می کنند.

پس از دانلود و اجرای برنامه، شما باید زبان مورد نظر را انتخاب کنید و پس از آن بلافاصله می توانید کامپیوتر را اسکن کرده و از وجود بد افزارهای احتمالی مطلع شوید. در بعضی موارد بد افزارها در قالب یک آنتی ویروس مانند AntiviruseLive بر روی سیستم شما نصب می شوند و ویروس هایی را بر روی کامپیوترتان شناسایی می کنند، این در حالی است که هیچ ویروسی بر روی سیستم وجود ندارد.

جالب اینکه بد افزارها با چنین حقه ای برای پاک کردن ویروس های خیالی از شما درخواست پرداخت هزینه هم می کنند.

پاک کردن این بد افزارها کار راحتی نیست، زیرا این برنامه ها اغلب جلوی حذف خود را می گیرند. اما شما به راحتی با استفاده از این نسخه پرتابل می توانید بر آن ها غلبه کنید.

کاربران ویندوز می توانند این نرم افزار رایگان را از طریق این آدرس دانلود کنند.

نکاتی که برای جلوگیری از نصب جاسوس افزارها لازم است بدانید و رعایت کنید

- هنگام گشت و گذار در وب گوش به زنگ باشید. مواظب پنجره های مرورگر که به شکل خودکار باز می شوند، باشید و قبل از آنکه از روی عادت گزینه Yes یا اوکی را انتخاب کنید، متن آن را با دقت بخوانید. در صورتی که صفحه ی باز شده با کاری که در حال انجام آن هستید ارتباطی نداشت یا اینکه به درستی متوجه منظور آن نشدید، با زدن دکمه ضربدر در سمت بالا و راست صفحه نسبت به بستن آن اقدام کنید. برای این کار از دکمه ی کنسل داخل صفحه استفاده نکنید. با این کار یکی از حقه های معمول بد افزارها برای نصب شدن بر روی کامپیوترتان با شکست مواجه می شود.
- جهت افزایش امنیت مرورگر اینترنتی تان جلوی اجرای خودکار و نصب برنامه های بالقوه خطرناک وب سایت ها را بگیرید. اگر از مرورگر فایرفاکس استفاده می کنید، بهترین راه نصب افزونه No Script است.
- هرگز به برنامه های کوچکی که توسط وب سایت های ناشناس و مشکوک پیشنهاد می گردند، اجازه نصب ندهید. فقط و فقط از وب سایت های معتبر و قابل اطمینان، نرم افزار دانلود کنید.
- تعداد زیادی از نرم افزارها هنگام نصب به همراه خود تبلیغ افزار نصب می کنند. قوانین هنگام نصب را بخوانید تا از وجود چنین نرم افزارهایی مطلع شوید. تایید کردن هر چیزی عواقب بدی دارد.

- با مهمترین نرم افزارهای آلوده به جاسوس افزار آشنا شوید. بیشترین فایل هایی که در اینترنت به این بد افزارها آلوده هستند شامل نرم افزارهای به اشتراک گذاری فایل، اسکرین سیورها، نرم افزارهای تغییر دهنده ی Wallpaper، اسمایلی های قابل دانلود و نرم افزارهای زیبا کننده نشانگر موس هستند. یکی دیگر از منابع جاسوس افزارها، سایت های ویژه بزرگسالان هستند.

درس هشتم – دیوار آتش و لزوم استفاده از آن

احتمالا تا به حال کلمه فایروال (Firewall) یا دیواره آتش را زیاد شنیده باشید. اما بسیاری از ما هنوز درک درستی از چیستی و فایده آن نداریم. به همین دلیل بهتر است قبل از هر چیزی به معرفی فایروال بپردازیم. در یک تعریف پایه و نسبتا کامل می توان گفت: فایروال یک برنامه نرم افزاری و یا قطعه سخت افزاری قابل نصب بر روی کامپیوتر است که می تواند از حمله به سیستم، هنگام استفاده از اینترنت، جلوگیری کند. فایروال (دیوار آتشین) اولین برنامه ای است که اطلاعات ورودی را می بیند. همچنین این برنامه آخرین بدرقه کننده اطلاعات (دیتاها) هنگام خروج از کامپیوتر است. همانند یک گارد امنیتی، جلوی ورودی ساختمان می ایستد و تصمیم می گیرد چه افرادی وارد شوند و چه کسانی حق خروج دارند. فایروال تمامی اطلاعات ورودی و خروجی را دریافت، بازرسی و بر حسب مورد از عبور آنها جلوگیری می کند.

حمله به کامپیوتر شما از روش های مختلفی انجام می شود. برای مثال این حمله می تواند یک فایل مثلا صوتی یا تصویری باشد که هنگام اجرا باعث بسته شدن و کرش نرم افزار پخش صدا و تصویر کامپیوتر می شود. اما در حقیقت با چنین شکل اجرا شدن، یک در پشتی (Back Door) بر روی سیستم ایجاد می شود که در واقع یک راه دسترسی به کامپیوترتان خواهد بود.

برخی اوقات هم ممکن است حمله به صورت درخواست های پیاپی برای انجام یک کار خاص از طرف یک کامپیوتر آلوده باشد که می تواند باعث قفل و کرش کردن سیستم عامل تان شود. به این شیوه، حمله ی DoS می گویند. برای جلوگیری از این حملات لازم است که ایرادهای امنیتی سیستم عامل و برنامه های کاربردی تان توسط برنامه نویسان آنها کنترل و بسته شوند. اما گاهی پیش می آید که قبل از توسعه دهنده و نویسنده برنامه، یک هکر به چنین باگ ها و سوراخ های امنیتی ناشناخته ای بر می خورد و از آنها حداکثر سوء استفاده را می کند.

کار فایروال این است که سوراخ های امنیتی شناخته شده را ببندد و تا حد امکان طبق الگوریتم های مشخص جلوی نفوذ از طریق نقاط آسیب پذیر ناشناخته سیستم را هم بگیرد. سیستم کاری فایروال به دو شیوه است: یکی فایروال داده های ورودی یا Inbound Firewall که اجازه ورود اطلاعات تایید نشده به شبکه را نمی دهد، تا کد مخربی وارد شبکه نشود. دیگری فایروال داده های خروجی یا

Outbound Firewall است که اجازه خروج اطلاعات غیر معمول از شبکه به اینترنت یا شبکه دیگر را نمی دهد، زیرا فرض بر این است که همه ی کامپیوترها آلوده اند و اطلاعات خروجی توسط بدافزارها تولید و ارسال می گردند. البته برای امنیت بیشتر، استفاده از فایروال هایی با هر دو قابلیت توصیه می شود.

توجه داشته باشید که فایروال ها بی نقص و عالی عمل نمی کنند و نمی توانند جلوی همه ی خطراتی که کامپیوتر شما را به یک قربانی فعالیت های خرابکارانه تبدیل می سازد، بگیرند. اما تا حد بسیار زیادی شانس خرابکارها را کم کرده و شما را از بسیاری خطرات نجات می دهند.

انواع مختلف فایروال های سخت افزاری معمولا فقط در مراکز بزرگ اداری، تجاری و یا امنیتی مورد استفاده قرار می گیرند و معمولا به دلیل قیمت بالا و شیوه ی کاربری دشوار، برای استفاده های شخصی و کاری کوچک عملا کاربردی ندارند. به همین دلیل در اینجا فقط به معرفی و ذکر خصوصیات برخی از فایروال های نرم افزاری می پردازیم که نسخه رایگان هم داشته باشند.

اولین توصیه ما برای مقابله با حملات اینترنتی استفاده از فایروال خود سیستم عامل است. ویندوز ایکس پی، ویستا و ۷ همراه با نسخه رایگانی از فایروال مایکروسافت عرضه شده اند که امنیت مناسبی را برایتان فراهم می کنند. فقط حواس‌تان باشد که هیچ‌گاه آنها را غیر فعال نکرده و یا در صورت عدم آگاهی لازم، تنظیمات پیش فرض شان را تغییر ندهید.

در ویندوز از طریق قسمت کنترل پنل می توان در پنجره ی Security Center، فایروال را خاموش یا روشن کنید. برای انجام تنظیمات مورد نظر هم، در کنترل پنل، صفحه ی Windows Firewall را باز کنید.

اما اگر فکر می کنید به امنیتی بیش از فایروال داخلی ویندوز نیاز دارید، برنامه های رایگان فراوانی در اختیار شما هست که به دو مورد از نمونه های واقعا خوب آن اشاره خواهیم کرد. ضمن اینکه بد نیست بدانید بعضی شرکت های امنیتی به همراه برخی نسخه های نرم افزارهای آنتی ویروس، یک دیوار آتشین هم قرار داده اند تا یک مجموعه امنیتی را در قالب یک نرم افزار داشته باشید.

در کامپیوترهای مک می‌توانید از Firewall پیش‌فرض در این سیستم عامل استفاده کنید که بسیار قوی است.

ZoneAlarm: یکی از بهترین برنامه های فایروال که تقریبا در بین بقیه رقبا منحصر به فرد عمل می کند، ZoneAlarm است. این نرم افزار در نسخه های مختلف برای کاربردهای متفاوتی تولید شده و نسخه رایگان آن هم از طریق این آدرس قابل دریافت است.

این برنامه با استفاده از چند سرویس امنیتی به هم پیوسته حمایت کامل و جامعی را برای سیستم تان فراهم می آورد. این برنامه شامل یک فایروال، نرم افزار کنترل برنامه ها، و قفل اینترنتی است که به شکل پویا و روانی سطوح امنیتی و دسترسی مختلفی را برای تان فراهم می آورد.

امکان قفل اینترنتی آن می تواند هنگامی که از اینترنت استفاده نمی کنید و یا پای کامپیوترتان نیستید، دسترسی آن به اینترنت را قطع کند. این ویژگی را هم می توان به صورتی تنظیم کرد که با شروع محافظ صفحه ی نمایش فعال شود و هم می توان مدت زمان بدون استفاده ماندن کامپیوتر را تعیین کرد تا ارتباط را به صورت خودکار قطع کند. این برنامه همچنین با کنترل دائمی سیستم عامل، مواظب فعالیت برنامه ها و دسترسی آنها به اینترنت است و بدون اجازه شما هیچ برنامه ای امکان اتصال به اینترنت را ندارد. همچنین هنگامی که فردی برای دست یابی به سیستم شما تلاش می کند، Zone Alarm، شما را مطلع کرده و آی پی مورد استفاده وی را هم در اختیارتان می گذارد.

Comodo: این برنامه به راحتی نصب شده و تنظیمات چندان پیچیده ای هم ندارد. کومودو یکی از بهترین برنامه های امنیتی است که به صورت رایگان عرضه شده و برنده بسیاری از جوایز بوده است. این فایروال با سیستم بسیار جالب و موثری به نام DDP با برنامه های نصب شده بر روی سیستم عامل برخورد می کند، به گونه ای که اگر نرم افزاری را نشناخت و یا از امنیت دسترسی آن به اینترنت مطمئن نبود، آن را در لیست برنامه های متخاصم قرار داده و از دسترسی آن به شبکه و اینترنت جلوگیری می کند. با این کار توان مقابله با بسیاری از تهدیدات و ضعف های ناشناخته ی امنیتی را هم به دست آورده است که حتی هنوز به عنوان یک باگ امنیتی نیز شناسایی نشده اند. کومودو به صورت خودکار به روز رسانی می گردد و همچنین امکان شخصی سازی تنظیمات و شیوه اعلام اخطارها را برای تان فراهم می کند. دانلود کنید...

یکی از سوالاتی که ممکن است برای بسیاری مطرح باشد، این است که آیا علیرغم به روز بودن تمامی برنامه ها و سیستم عامل، باز هم نیازی به استفاده از فایروال است؟

پاسخ این است که مطمئنا شما به استفاده از فایروال نیاز دارید، زیرا ممکن است حتی با نصب همه آپدیت های امنیتی و به روز رسانی سیستم، باگ و نقاط آسیب پذیری در برنامه ها و سیستم عامل کشف شود که عرضه بسته و به روزرسانی امنیتی آن روزها و حتی ماه ها طول بکشد. حتی برخی از هکرهای زرنگ همان روز کشف و اعلام یک ایراد امنیتی، از آن سوءاستفاده کرده و کامپیوترها را مورد حمله قرار می دهند. از طرف دیگر فایروال ها به عنوان نگهبان های درهای ورودی و خروجی اطلاعات می توانند یک مرحله امنیت کامپیوتر شما را ارتقاء دهند.

در کنار آن شرکت های سازنده فایروال بسیار سریع تر از شرکت های توسعه نرم افزار می توانند در مقابل یک آسیب پذیری عکس العمل نشان دهند، زیرا تنها کافی است که به بخش آسیب پذیر و برنامه های مرتبط با آن اجازه تبادل اطلاعات با شبکه و اینترنت را ندهند. همچنین فایروال با جلوگیری از هرگونه تبادل اطلاعات مشکوک، در بسیاری از مواقع جلوی وارد آمدن آسیب از طریق ایرادهای نرم افزاری که بعدها شناخته و حل می شوند را می گیرد.

به طور خلاصه فراموش نکنید که فایروال ها از اجزای بسیار مهم و جدایی ناپذیر برای حفظ امنیت شما هستند و داشتن یک فایروال فعال و به روز هیچ گاه نباید فراموش شود. اگر در کار با کامپیوتر و اینترنت مبتدی هستید، توصیه می کنیم که از فایروال داخلی خود سیستم عامل ویندوز استفاده کنید. همین الان آن را بررسی کنید تا از فعال بودنش اطمینان حاصل کنید. اگر اطلاعات بیشتری دارید می توانید از فایروال کومودو که در این درس معرفی شد، استفاده کنید و یا اگر تنظیمات بیشتری نیاز دارید و کمی حرفه ای تر هستید استفاده از Zone Alarm را به شما توصیه می کنیم.

درس نهم – مبانی امنیت در سیستم عامل ویندوز

یک سیستم عامل مثل یک مرکز فرماندهی به شما اجازه افزایش یا کاهش امنیت و سطوح دسترسی کامپیوترتان را می دهد. سیستم عامل ویندوز به داشتن نقاط آسیب پذیر فراوان مشهور است، اما اگر نخواهید سیستم عامل دیگری (مانند لینوکس) نصب کنید، باید یک آگاهی اولیه در مورد روش های بالا بردن امنیت کامپیوتر داشته باشید. تنظیمات امنیتی ویندوز تا زمانی که بر روی حالت پیش فرض هستند هیچ امنیتی ندارند و جهت تاثیرگذاری در امنیت باید شخصا آنها را فعال کنید.

امنیت سیستم عامل نقش تعیین کننده ای در امنیت کامپیوتر دارد و با توجه به گسترش جهانی سیستم عامل ویندوز در این درس به امنیت ویندوز می پردازیم. اهمیت این مطلب زمانی آشکار می شود که بدانیم ویندوز، علی رغم گسترش بیشتر نسبت به رقیبان خود (لینوکس و مک) امنیت کمتری دارد.

عوامل مختلفی بر روی امنیت سیستم عامل تاثیرگذار بوده و در نهایت در امنیت و حفاظت فایل ها و اطلاعات شخصی ما دخیل هستند. در این درس توضیحاتی در خصوص اصولی که برای امنیت ویندوز ضروری هستند پرداخته شده که دانستن آنها برای حفاظت کامپیوتر ضروری است.

به روز رسانی (Update)

سیستم عامل ویندوز، بهشتی برای سازندگان بدافزارها است و برای جلوگیری از خطراتی که شما و سیستم عامل تان را تهدید می کند، به روز رسانی حداقل کار ممکن است. بهتر است به طور مکرر ویندوز خود را آپدیت کنید. مایکروسافت به شدت بر روی به روز رسانی ویندوز سخت گیری می کند و برای اینکه کاربران به آسانی بتوانند به روزرسانی را انجام دهند، از Windows Update استفاده می کند. صرف نظر از این که شما از چه ویندوزی استفاده می کنید، باید سیستم تان را به گونه ای تنظیم کنید که این فرآیند به صورت خودکار انجام شود.

برای به روزرسانی خودکار و راحت ویندوز، می توانید Windows Update را بر روی Install Updates Automatically قرار دهید. البته لازم است زمان به روزرسانی را با توجه به کار خود و زمان اتصال سیستم به اینترنت، به گونه ای برنامه ریزی کنید که بسته های به روزرسانی مهم را از دست ندهید.

سیستم آپدیت ویندوز به گونه ای است که حتی با سرعت پایین اینترنت هم به خوبی کار کرده و به ندرت دچار مشکل می شود. اما برای اجتناب از این مورد، می توانید Windows Update را بر روی حالتی قرار دهید که بسته های به روز رسانی را دانلود کرده، ولی آن ها را بدون اجازه شما نصب ننماید (download but not install the files)؛ با این کار می توانید به روز رسانی های ضروری را سریعا دریافت نمایید، اما قبل از نصب آن ها کمی جستجو نموده و در صورت اطمینان از کارکرد درست، اجازه نصب آنها را بدهید. با این کار، مواردی را هم که نمی خواهید نصب شوند، از دست نمی دهید و در لیست انتظار باقی می مانند.

به یاد داشته باشید، در صورتی که شما Windows Update را فعال ننموده اید، هم اکنون زمان آن رسیده که این کار را انجام دهید. برای این کار می توانید به راحتی در صفحه کنترل پنل، Windows Update را یافته، اجرا و آن را فعال نمایید. این عمل به حیات و امنیت سیستم شما بستگی دارد، پس آن را پشت گوش نیاندازید.

نکته: چند سالی است که مایکروسافت برای شناسایی ویندوزهای غیر اصل که به صورت غیرقانونی در اختیار کاربران قرار می گیرند، اقدام به نصب نرم افزار Windows Genuine Advantage می کند. این نرم افزار قبل از آپدیت ویندوز بر روی آن نصب شده و در صورتی که ویندوز شما اورجینال تشخیص داده نشود، اخطارهای آزار دهنده ای را نمایش می دهد. به همین دلیل بسیاری از کاربران ایرانی که از ویندوزهای غیر اصل استفاده می کنند، برای اینکه این نرم افزار مشکلی برایشان به وجود نیاورد، از به روز رسانی ویندوز اجتناب می کنند. اما با کمی جستجو در اینترنت می توان راه ها و نرم افزارهایی ساده برای رفع این مشکل یافت. بنابراین تحت هیچ شرایطی از آپدیت ویندوز خودداری نکنید.

در کنار آپدیت ویندوز می توانید با استفاده از Windows Update نرم افزارهای مجموعه آفیس و ویندوزلایو و شاید نرم افزارهای دیگری که مربوط به مایکروسافت هستند را نیز آپدیت کنید، اما این کافی نیست و برای به روز رسانی سایر نرم افزارهای مورد استفاده شما کاربردی ندارد.

به یاد داشته باشید، همه نرم افزارهایی که در سیستم عامل خود استفاده می کنید، به صورت بالقوه خطراتی را متوجه سیستم عامل شما می کنند. به منظور کاهش ریسک خطرپذیری این نرم افزارها،

لازم است آخرین بسته های به روز رسانی آنها را نیز دریافت کرده و نصب نمایید. اما به روز رسانی تک تک نرم افزارهایی که بر روی سیستم خود دارید، بسیار خسته کننده و ملال آور است؛ علاوه بر اینکه ممکن است آپدیت برخی از آنها را از قلم بیاندازید.

برای حل این مشکل، می توانید از نرم افزاری که سایت FileHippo.com در اختیار شما قرار داده، استفاده کنید. این برنامه نرم افزارهای نصب شده بر روی سیستم شما را بی وقفه بررسی و با بانک اطلاعاتی عظیم خود تطبیق می دهد. در صورتی که نسخه جدیدی برای یکی از برنامه های سیستم شما عرضه شده باشد، شما را مطلع می کند.

این برنامه رایگان بوده و تنها ۲۰۰ کیلوبایت حجم دارد. همچنین حجم بسیار اندکی را در حال اجرا اشغال می کند. لازم است بدانید که FileHippo بهترین نرم افزار برای آگاهی از زمان به روزرسانی برنامه ها است. ضمنا سایت FileHippo یکی از بزرگترین منابع قابل اعتماد برای نسخه های قدیمی و جدید بسیاری از برنامه های ویندوزی است. برای دانلود این نرم افزار می توانید به این آدرس مراجعه کنید.

در کنار FileHippo، برای بررسی دقیق نرم افزارهایی که نیاز به آپدیت دارند، می توانید از نرم افزار Secunia PSI نیز استفاده کنید. این نرم افزار علاوه بر آگاهی رسانی در مورد نرم افزارهایی که نیاز به آپدیت دارند، آنها را براساس اهمیت لیست می کند. برای مثال یک آپدیت کوچک در نرم افزار Pidgin، به اندازه ی یک بسته ی به روزرسانی در اینترنت اکسپلورر اهمیت ندارد. پس زمانی که شما با استفاده از Secunia سیستم تان را اسکن می کنید، به شما اعلام می کند که کدام نرم افزار نیاز به آپدیت دارد، آخرین باری که نرم افزار مورد نظر آپدیت شده کی بوده و همچنین بسته ی به روزرسانی مورد نظر از نظر کارکرد و امنیت تا چه اندازه مهم و ضروری است. می توانید برای دانلود این نرم افزار رایگان از این آدرس استفاده کنید.

استفاده از آخرین نسخه ویندوز

برای افزایش امنیت کامپیوتر خود، علاوه بر به روز رسانی ویندوز، بهتر است از آخرین نسخه ویندوز استفاده کنید. اگر از ایکس پی یا ویستا استفاده می کنید، توصیه می شود آن را به ویندوز ۷ ارتقا دهید.

این عمل را در استفاده از نرم افزارهای مورد استفاده خود نیز مد نظر قرار دهید. ترجیحا آخرین نسخه از نرم افزارهای مورد نیاز خود را بر روی کامپیوتر نصب نمایید و نرم افزارهای قدیمی را ارتقا دهید.

قرار دادن رمز عبور بر روی حساب های کاربری

یکی از مهمترین نکاتی که باید در رابطه با استفاده از ویندوز رعایت کنید، قرار دادن رمز عبور بر روی حساب های کاربری ایجاد شده در ویندوز است. اگر تنها خودتان از کامپیوتر استفاده می کنید، بهتر است یک حساب جدید با دسترسی های ادمین ساخته و به جای استفاده از اکانت Administrator از آن استفاده کنید و اگر به غیر از شما افراد دیگری نیز از سیستم استفاده می کنند، می توانید برای هر یک، یک حساب جداگانه بسازید. بهتر است هر حساب نیز رمز عبوری مختص خود داشته باشد و تا حد امکان تنها یکی از حساب ها به همه قسمت های سیستم دسترسی کامل داشته باشد.

برای رمزگذاری بر روی یک حساب می بایست ابتدا از منوی Start، صفحه ی Control Panel را باز کنید، سپس در آنجا به حساب کاربران (User Accounts) بروید و در پنجره ای که باز می شود در قسمت pick an account to change بر روی نام کاربری خود کلیک کنید. در پنجره جدید بر روی Create a password کلیک کنید. حال رمزعبور خود را در کادر اول بنویسید و در کادر دوم آن را تکرار کنید. حال دکمه Create password را بزنید، سپس دکمه ی Yes, Make Private را کلیک کنید. حالا حساب کاربری شما رمز عبور دارد و فایل هایی که در پوشه Documents and Settings هر کاربر ذخیره می شوند، تنها توسط آن کاربر و ادمین سیستم قابل دسترسی هستند.

هنگامی که قصد ترک موقتی کامپیوتر خود را- حتی برای چند لحظه- دارید، آن را قفل نمایید تا فرد دیگری به آن دسترسی نداشته باشد. برای قفل کردن کامپیوتر می توانید کلیدهای ترکیبی ویندوز و L را از صفحه کلید فشار دهید.

همچنین بهتر است برای زمانی که ویندوز در حالت اسکرین سیور (محافظ صفحه نمایش) است و می خواهید به میز کار برگردید نیز، رمز عبور تعیین کنید. برای این کار می توانید با مراجعه به تنظیمات محافظ صفحه نمایش، تیک گزینه On resume, Protect Password را بگذارید.

اهمیت نظم در ذخیره سازی فایل ها و فولدرها

فایل ها و فولدرهایی که در ویندوز ذخیره یا ایجاد می کنید، اهمیت ویژه ای دارند. با توجه به افزایش روز افزون حجم هارد دیسک ها، شاید مسخره باشد که بخواهیم از موجودیت و مکان تک تک فایل هایی که در کامپیوتر ذخیره کرده ایم، آگاه باشیم. اما لازم است تا جایی که ممکن است منظم باشید. مثلا برای یافتن یک فایل ویدئویی در میان انبوهی از فایل ها و فولدرهای مختلف به جستجو نپردازید؛ یا فولدرهای خود را با نام New Folder رها نکنید. این امر باعث می شود که بد افزارها و برنامه های مخرب نتوانند در هارد به هم ریخته تان مخفی شوند و شما هم بی خبر بمانید. سعی کنید هر چند وقت یک بار که اتاق خود را مرتب می کنید، پوشه ها و فایل های کامپیوتر خود را نیز مرتب کنید.

نمایش پسوند فایل ها در ویندوز

در همه ی سیستم عامل ها، فایل های مختلف پسوند مشخصی (که اغلب سه حرفی است) دارند که به شناسایی آنها توسط کاربران و نرم افزارها کمک می کند. مثلا بیشتر فایل های تصویری پسوند jpg و gif دارند، یا فایل های متنی اغلب با پسوند txt و doc ذخیره می شوند. در ویندوز به صورت پیش فرض پسوند فایل ها مخفی است و به کاربر نشان داده نمی شود که این قابلیت، ظاهر فایل ها را برای کاربر زیبا و جذاب تر کرده و همچنین از سردرگمی کاربران مبتدی جلوگیری می کند. اما در پشت این قابلیت، نکته ای امنیتی مهمی پنهان مانده است که باید به آن دقت کرد.

فرض کنید که کاربر هنگام نصب یک نرم افزار، فایلی تحت نام readme را بدون آنکه از پسوند و محتوایش آگاه باشد، باز کند. وی با این کار عملا به استقبال خطر رفته است؛ چرا که ممکن است پسوند این فایل به جای readme.txt به صورت readme.txt.bat باشد، که bat به خاطر مخفی بودن پسوندها در ویندوز، از دید کاربر پنهان مانده است. دوبار کلیک بر روی این فایل (که در حقیقت یک فایل اجرایی است)، احتمال دارد منجر به اجرای مستقیم کد مخرب در سیستم کاربر گردد.

برای نمایش پسوند فایل ها در ویندوز ایکس پی، My Computer را باز کرده و از منوی Tools گزینه ی Folder Options را انتخاب نمایید. در پنجره باز شده تب View را کلیک کنید و از لیست موجود تیک گزینه Hide extensions for known file types را بردارید و دکمه OK را در پایین پنجره کلیک کنید.

در ویندوز ویستا و ۷ نیز می توانید پس از باز کردن Computer، از منوی Organize گزینه Folder and search options را انتخاب کرده و در پنجره باز شده همانند ویندوز ایکس پی تب View را انتخاب کرده و تیک گزینه Hide extensions for known file types را بردارید و بر روی OK کلیک کنید.

توجه: پس از اعمال تنظیمات و نمایش پسوند فایل ها، دقت کنید که هنگام تغییر نام فایل ها، پسوند آنها را حذف نکنید و یا تغییر ندهید. در این صورت ویندوز با شناسایی فایل مورد نظر و اجرای آن دچار مشکل می شود.

تنها نرم افزارهای ضروری را نصب کنید

علاوه بر نرم افزارهایی که به صورت پیش فرض در ویندوز وجود دارند، نرم افزارهای دیگری نیز برای انجام اموری خاص، مورد نیاز هستند. اما زمانی که یک نرم افزار جدید نصب می کنید، درست مثل این است که در حال خوردن غذا هستید. همان طور که ممکن است یک غذای مضر و یا تاریخ گذشته شما را مسموم کند، نرم افزارهای مضر و به روز نشده هم می توانند کامپیوتر شما را مسموم کنند. پس هنگام نصب یک نرم افزار، راجع به منتشر کنندگان آن تحقیق کنید و میزان قابل اعتماد بودن آنها را برآورد کنید. به طور معمول بسیاری از نرم افزارها نقص های (Bug) امنیتی زیادی دارند که ویندوز نمی تواند همه آنها را حل کند. پس هرگز یک نرم افزار غیر ضروری که مثلا میزکار شما را زیباتر می کند و یا اینکه شکل آن را تغییر می دهد، نصب نکنید. مثلا اگر تنها استفاده شما از کامپیوتر خواندن ایمیل و تایپ متون است، به جز یک مرورگر و نرم افزار ویرایشگر متن به چیز دیگری نیاز ندارید، پس برنامه دیگری نصب نکنید.

در صورتی که کامپیوتر خود را به تازگی خریداری کرده اید، احتمالا تعدادی نرم افزار توسط فروشنده بر روی آن نصب شده است، ولی به خاطر داشته باشید که این کار از نظر امنیتی چندان مطلوب نیست. اگر شما دسترسی نامحدود و ارزان قیمت به اینترنت داشته باشید، تمام احتیاجات شما فقط یک CD ویندوز خواهد بود. تمام نرم افزارهای مورد نیاز شما به صورت رایگان می توانند از اینترنت تهیه شوند. پس اگر ویندوز امن و مطمئنی می خواهید، بهتر است همه درایوهای کامپیوتر را پاک کرده و ویندوزی جدید را بر روی کامپیوتر نصب کنید. پس از آن نیز در وهله ی اول تنها نرم افزارهای

امنیتی و حفاظتی که از آنها مطمئن هستید، نصب کنید و پس از آن به دانلود و نصب نرم افزارهای مورد نیاز خود بپردازید.

هنگام وب گردی با تبلیغ های مختلفی مواجه می شوید که شما را ترغیب به دانلود و نصب نرم افزارهای مختلفی می کنند. یک تولبار قدرتمند، یک آنتی ویروس خوب و رایگان، دسترسی رایگان به سایت های پولی و... . هرگز، هرگز و هرگز یک نرم افزار ناشناس را دانلود و نصب نکنید. سعی کنید فقط از منابع قابل اعتماد فایل دانلود کنید و به سایت های دیگر اعتماد نکنید. این نرم افزارها یکی از اصلی ترین روش ها برای آلوده کردن سیستم عامل هستند. شما یک تولبار مفید نصب می کنید و در کنار آن به صورت مخفیانه یک جاسوس افزار بر روی کامپیوترتان جا خوش می کند. تا به حال از کند شدن کامپیوتر شاکی شده اید؟ یکی از دلایل اصلی کاهش سرعت کامپیوتر، آلودگی با بد افزارهای مختلف است. بنابراین نسبت به کاهش سرعت سیستم عامل تان حساس باشید و آنها را با نرم افزارهای مناسبی که در بقیه درس های این دوره معرفی شده است اسکن کنید.

سراغ نرم افزارهای P2P نروید

نرم افزارهای به اشتراک گذاری فایل یا P2P به طور گسترده توسط کاربران برای دانلود نرم افزار، فیلم و موسیقی به کار می روند و یکی از بهترین منابع برای دسترسی به فیلم رایگان و نرم افزارهای کرک هستند. این شبکه ها یکی از منابع اصلی برای انتشار بد افزارها محسوب می شوند. به طور کلی توصیه می کنیم که از این نرم افزارها بر روی کامپیوترتان استفاده نکنید. به خصوص در کامپیوترهای اداری و محل کار. اما اگر به هیچ عنوان نمی توانید از آنها دل بکنید، حداقل سعی کنید در کامپیوتر خانگی تان پیش نیازهای امنیتی را به طور کامل و با دقت رعایت کنید. در عین حال باید بدانید که از چه نرم افزار P2P استفاده می کنید، چرا که بسیاری از این نرم افزارها خودشان حاوی جاسوس افزار یا تبلیغ افزار هستند. بنابراین پیش از نصب یکی از آنها، خوب در موردش تحقیق کنید.

از نسخه های ۶۴ بیتی ویندوز استفاده کنید

اگر سخت افزار قدرتمند و مورد نیاز را دارید، توصیه می کنیم از نسخه ۶۴ بیتی سیستم عامل ویندوز استفاده کنید چرا که تعدادی امکان امنیتی در این نسخه وجود دارد که نسبت به نسخه ی ۳۲ بیتی امنیت بیشتری برای شما فراهم می کند.

اهمیت نصب نرم افزارهای نابودگر بد افزارها

علاوه بر مطالبی که در خصوص امنیت ویندوز و آسیب پذیری آن اشاره شد، نصب نرم افزارهایی که در مقابله با بد افزارها به یاری ویندوز بشتابند، اجتناب ناپذیر است. نرم افزارهای ضد ویروس، ضد جاسوس افزار و ضد بد افزار در کنار یک فایروال مناسب که فعالیت ها و ارتباطات شبکه را مدیریت می کند، برای امنیت کامپیوتر ضروری است. با این نرم افزارها و اهمیت نصب آنها در سایر درس های این دوره آشنا می شوید.

پاکسازی نرم افزارهای نصب شده

بسیاری از نرم افزارهایی که بر روی سیستم خود نصب می کنید، برای اجرا و در اختیار قرار دادن کلیه امکانات نرم افزار، فایل هایی را در قسمت های مختلف کامپیوتر کپی و اغلب تغییراتی را در رجیستری ویندوز ایجاد می کنند.

در صورتی که قصد پاک سازی نرم افزاری را داشته باشید و این کار را از طریق Add/Remove در ویندوز انجام دهید، بسیاری از فایل ها و تغییراتی که در ویندوز کپی و ایجاد شده اند، بدون تغییر باقی می مانند و نرم افزار مربوطه تنها Uninstall می شود. این رد پاها، می توانند به صورت بالقوه حفره های امنیتی خطرناکی باشند که توسط هکرها مورد سوء استفاده قرار گیرند.

اما برای پاک سازی کامل نرم افزارها و رد پاهایی که در ویندوز به جا گذاشته اند، می توان از نرم افزاری رایگان و کاربردی به نام Revo Uninstaller استفاده کرد. این نرم افزار علاوه بر Uninstall کردن نرم افزار مربوطه، با شناسایی رد پاها و فایل های اضافی و پاک سازی کامل آنها از ویندوز، امنیت بیشتری را برای کامپیوتر شما تامین می کند. دانلود کنید...

رمزنگاری اطلاعات سیستم عامل

چه اتفاقی رخ می دهد اگر وقتی پشت کامپیوتر نیستید، کسی سراغ آن برود و سعی کند وارد سیستم عامل شده و به اطلاعات دسترسی پیدا کند؟ آیا می دانید حتی اگر بر روی ویندوز رمز عبور قرار داده باشید، باز هم ورود به آن کار سختی نخواهد بود؟ با یک توزیع زنده لینوکس می توان کامپیوتر را بوت کرد و به فایل های شما دسترسی داشت. در یک روش دیگر می توان با استفاده از یک سی دی نجات، پسورد ویندوز را ریست کرد و با یک پسورد جدید وارد کامپیوتر شد! راه بعدی

استفاده از روش Brute Force و کرک کردن پسورد است. بنابراین همانطور که می بینید راه های مختلفی برای دسترسی غیر مجاز به سیستم عامل تان وجود دارد. چگونه جلوی آنها را بگیریم؟

برای این کار باید اطلاعات را رمزنگاری کنید. سیستم عامل ویندوز در نسخه ویستا و ۷ امکان جدیدی به نام BitLocker دارد که از طریق آن می توان کل پارتیشن سیستم عامل را رمزنگاری کرد (معمولا پارتیشن C جایی است که ویندوز نصب شده است). با فعال کردن بیت لاکر تمام اطلاعات بر روی این درایو رمز نگاری می شوند. دقت کنید که این کار شامل درایوهای دیگر نیست. بنابراین فایل های مهم را بر روی همین درایو نگه داری کنید. ضمنا باید بدانید این امکان بر روی همه نسخه های ویندوز ۷ و ویستا وجود ندارد. با استفاده از بیت لاکر می توانید مطمئن باشید در صورت دسترسی غیرمجاز به کامپیوتر یا سرقت اطلاعات، امکان مشاهده آنها وجود ندارد. اما این روش در صورت استفاده از Brute Force برای پیدا کردن رمز عبور سیستم عامل جواب نمی دهد. برای مقابله با آن باید رمز عبور بسیار مستحکمی داشته باشید. بنابراین استفاده از بیت لاکر در ترکیب با یک رمز عبور بسیار قوی برای ویندوز (بالاتر از ۱۴ کاراکتر) به شما این اطمینان را خواهد داد که اطلاعات شما در جای امنی نگه داری می شوند.

توجه: برای رمز نگاری اطلاعات در پارتیشن های دیگر و روش های مکمل در این دوره ی آموزشی با نرم افزار True Crypt در درس امنیت دیتا آشنا خواهید شد.

درس دهم – نگهداری و پاک کردن اطلاعات به صورت امن

در این مبحث قصد داریم تا امنیت اطلاعات را از حیث نحوه ی رفتار درست با اطلاعات مهم و محرمانه بررسی کنیم. همه افراد در سطوح مختلف خصوصی و کاری اطلاعاتی دارند که محرمانه و مهم تلقی می کنند و از اینکه در اختیار دیگران قرار بگیرد، احساس ناراحتی و خطر می کنند. این محتوای ارزشمند می تواند عکس های خانوادگی و نامه های شخصی باشد و یا هر گونه اطلاعات دیگر که نباید در دسترس دیگران قرار بگیرد.

در این درس ابتدا به راه های نگهداری اطلاعات به شیوه هایی امن و کم خطر می پردازیم و سپس راه درست نابودی اطلاعات را معرفی می کنیم. راه های مختلف سخت افزاری و نرم افزاری برای مقابله در برابر حملات احتمالی وجود دارد که استفاده توام از آنها و ایجاد لایه های مختلف امنیتی کار را برای افراد متجاوز سخت تر می کند.

به این نکته توجه داشته باشید که همیشه احتمال نفوذ افراد به کامپیوتر شما وجود دارد و در مواردی تمام اقدامات شما برای محافظت از خودتان بی اثر می شود. به این ترتیب رها کردن اطلاعات مهم و حساس بدون هیچ گونه حمایت، شما را در معرض خطرات جدی قرار می دهد. دو راه کلی برای حمایت بیشتر از اطلاعات در کامپیوتر وجود دارد؛ اول اینکه اطلاعات را با رمزگذاری برای سایرین غیر قابل فهم کرد و دوم اینکه آنها را از معرض دید دیگران پنهان کرد.

در این بخش به بررسی موارد زیر می پردازیم:

- چگونه اطلاعات را به صورت رمز در آورید؟
- خطرات نگهداری اطلاعات به صورت رمز
- چگونه از اطلاعات حافظه های جانبی که احتمال سرقت یا مفقود شدن آنها زیاد است، محافظت کنیم؟
- بررسی راه های مخفی کردن اطلاعات از متجاوزان فیزیکی و شبکه ای

اطلاعات خود را رمزگذاری کنید

اگر از رمز ورود ویندوز به عنوان تنها حامی اطلاعات محرمانه خود استفاده می کنید، اشتباه بزرگی را مرتکب شده اید، زیرا در صورتی که شخصی کامپیوتر شما را با استفاده از یک سی دی لایو راه اندازی کند، بدون هیچ دغدغه ای به کلیه ی پوشه های شما دسترسی خواهد داشت. در درس امنیت سیستم عامل ویندوز خواندید که با استفاده از بیت لاکر (BitLocker) می توان درایو ویندوز را رمزنگاری کرد و همچنین در سیستم عامل مک می‌توانید از Filefault که بصورت پیش‌فرض در سیستم وجود دارد استفاده کنید.

نرم افزارهایی مانند True Crypt فضایی شبیه به گاو صندوق را برای شما ایجاد می کنند که تنها افرادی که کلید مخصوص را داشته باشند به درون آن راه پیدا می کنند. البته دقت داشته باشید که تنها محتوای درون این محدوده از امنیت کامل برخوردار است و سایر اطلاعات از این امکان برخوردار نیستند. شما همچنین می توانید چنین فضای امنی را بر روی حافظه پرتابل خود نیز ایجاد کنید و فایل های مهم خود را درون آن فضا نگهداری کنید.

امکانات متعددی که True Crypt در اختیار شما می گذارد باعث شده است که این نرم افزار از جهات متعددی با سایر نرم افزارهای مشابه تفاوت داشته باشد.

نکاتی در مورد استفاده درست از رمزگذارها

نگهداری فایل های محرمانه و حساس همواره برای شما و اطرافیان تان خطرناک است، برای مثال ممکن است که اسناد فنی محرمانه شرکت تان را نگهداری می کنید که برای شرکت رقیب تان مهم است. استفاده از نرم افزارهای رمزگذار و سایر اقدامات امنیتی این خطر را تا حد زیادی کم می کند، اما هیچ گاه آن را کاملا از بین نمی برد. بنابراین اولین قدم در حفظ اطلاعات محرمانه، از بین بردن تمامی اطلاعاتی است که نگهداری آنها ضرورتی ندارد.

قدم دوم استفاده از یک نرم افزار رمزگذاری قوی مانند True Crypt است. برای استفاده درست از نرم افزارهایی مانند True Crypt همواره باید چند نکته ابتدایی را در ذهن داشته باشید. هر قدر هم این نرم افزارها از ساختار قوی برخوردار باشند، تا زمانی که شما این نکات را رعایت نکنید، نمی توانند موثر عمل کنند.

هر بار که شما برای استفاده از محیط امن نرم افزار، قفل آن را باز می کنید، امکان دسترسی را برای سایرین به وجود می آورید. بنابراین همواره دقت داشته باشید جز مواردی که به اطلاعات درون گاو صندوق تان (True Crypt) نیاز دارید، درب آن را بسته نگه دارید.

در اینجا به ذکر چند موقعیت می پردازیم که توجه ی بیشتر شما را برای بسته بودن قفل نرم افزار می طلبد:

- زمانی که از کامپیوتر خود برای مدتی هر چند کوتاه فاصله می گیرید: وقتی که شما کامپیوتر خود را رها می کنید، باید اطمینان حاصل کنید فایل های خود را در دسترس فیزیکی و یا غیر فیزیکی متجاوزان قرار نداده باشید. باز بودن True Crypt در این وضعیت به معنی تقدیم کردن محتوای رمز شده آن به هکرها است.
- قبل از قرار دادن کامپیوتر در حالت های Sleep و Hibernate و یا در زمان هایی که کامپیوتر خود را در اختیار افراد دیگر قرار می دهید، دقت کنید که از نرم افزار خارج شده باشید و کامپیوتر را خاموش کنید. زمان گذشتن از گیت های بازرسی از مواردی است که ممکن است به این نکته بی توجه باشید.
- قبل از اتصال یک حافظه جانبی ناشناس یا قرار دادن یک سی دی درون کامپیوتر حتی اگر متعلق به فردی باشد که کاملا به او اطمینان دارید، از بسته بودن برنامه اطمینان حاصل کنید.
- اگر شما با استفاده از نرم افزار، فضای امنی را بر روی یک کول دیسک ایجاد کرده اید، به یاد داشته باشید که تنها جدا کردن آن از کامپیوتر باعث خروج کامل از نرم افزار نمی شود و حتما باید قبل از جدا کردن حافظه از کامپیوتر نرم افزار را غیر فعال کنید. **جدا کردن بدون خروج از نرم افزار، علاوه بر ایجاد خطرات امنیتی، ممکن است باعث خرابی و از دست رفتن اطلاعات درون True Crypt شود.**
- اگر تصمیم دارید یک فضای امن بر روی حافظه ی فلش خود داشته باشید، توصیه می کنیم که یک نسخه پرتال از نرم افزار را نیز بر روی این حافظه کپی کنید تا در صورت نیاز بتوانید با استفاده از کامپیوترهای دیگر نیز به اطلاعات خود دسترسی داشته باشید. دقت کنید در

صورتی که یقین نداشتید که کامپیوتری که مورد استفاده قرار می دهید عاری از هر گونه Malware یا بد افزار است، از تایپ کردن رمز عبور خودداری کنید.

اطلاعات محرمانه و حساس خود را مخفی کنید

برخی از مردم بر این باورند که استفاده از نرم افزارهای رمزنگار باعث می شود که برچسب اتهام راحت تر بر آنها زده شود و بسیاری دیگر نیز با این دغدغه روبرو هستند که با استفاده از این نرم افزارها موقعیت فایل های محرمانه آنها به راحتی مشخص می شود. به هر ترتیب تنها دو دلیل اصلی می تواند باعث شود که شما برای استفاده از نرم افزار True Crypt دچار معذوریت باشید. خطر قرار گرفتن در معرض اتهام و یا مشخص شدن محل فایل های محرمانه شما.

اگر در چنین شرایطی قرار دارید شما چند انتخاب دارید:

استفاده از نرم افزارهای رمزنگار را کنار بگذارید و با استفاده از یک سیستم کد گذاری، بخش های اصلی اطلاعات خود را نگهداری کنید.

شما می توانید از تکنیکی که Steganography نامیده می شود برای مخفی کردن اطلاعات محرمانه استفاده کنید و دیگر نیازی به رمزنگاری آنها نداشته باشید. البته ابزارهایی نیز وجود دارند که می توانند این کار را برای شما ساده تر کنند، اما استفاده از آنها باید با دقت بالایی صورت گیرد تا مشخص نشود که شما از چه ابزاری استفاده کرده اید.

می توانید اطلاعات خود را در یک ایمیل امن نگهداری کنید. البته استفاده از این راه، مستلزم داشتن یک شبکه امن اینترنت است و همواره خطر به جا گذاشتن اطلاعات بر روی کامپیوتر در زمان تبادل آنها وجود خواهد داشت.

شما می توانید اطلاعات خود را بر روی یک حافظه جانبی و یا یک هارد دیسک پرتابل نگهداری کنید. اما این ابزارها بسیار بیشتر از کامپیوترها در معرض گم شدن و یا توقیف قرار دارند، به همین دلیل نگهداری اطلاعات محرمانه رمزنگاری نشده بر روی آنها به مراتب خطرناک تر است.

استفاده از تکنیک های فوق به صورت همزمان امنیت اطلاعات شما را بالا خواهد برد و حتی در چنین شرایطی که استفاده از نرم افزارهای رمزنگار خطر محسوب می شود، باز هم استفاده از True Crypt ارزشمند است.

اگر می خواهید گاو صندوق شما کمتر جلب توجه کند، می توانید آن را به شکل نوع دیگری از فایل تغییر نام دهید. مثلا می توانید از طریق پسوند «iso» فایل را یک ایمیج (Image) آماده ی رایت CD جلوه دهید. البته به حجم فایل دقت داشته باشید که از این ترفند برای فایل هایی با حجم حدود MBV۰۰ استفاده کنید. این حرکت تا حدی شبیه این است که شما گاو صندوق اتاق کار خود را پشت تابلوی نقاشی پنهان می کنید.

حتی این امکان برای شما فراهم است که خود نرم افزار True Crypt را نیز تغییر نام دهید و آن را به شکل موجه دیگری بر روی USB و یا هارد دیسک خود نگهداری کنید. در زمان نصب نرم افزار در قسمت True Crypt Guide توضیحات لازم برای انجام این کار به شما داده می شود.

خطر مشخص شدن موقعیت اطلاعات محرمانه

نگهداری کلیه اطلاعات محرمانه در یک محل نیز خطراتی را به همراه دارد. در شرایطی که به دلیل تهدید شدن و یا هر عامل مشابه دیگری، مجبور به ارائه رمز عبور خود می شوید، به راحتی تمامی اسرار شما فاش می شوند.

برای جلوگیری از این مشکل، نرم افزار True Crypt امکانی را در اختیار شما قرار می دهد که به وسیله ی آن شما می توانید اطلاعات را براساس اهمیت و درجه محرمانگی طبقه بندی کنید. این نرم افزار با ایجاد یک بخش مخفی درون گاو صندوق که فقط شما از وجود آن مطلع هستید، فضای مناسبی را برای نگهداری فایل های خیلی محرمانه شما به وجود می آورد. در زمانی که رمزعبور True Crypt شما به هر دلیلی در اختیار افراد متجاوز قرار گیرد، می توانید همچنان از اطلاعات خود محافظت کنید و در این حالت تنها اطلاعات لایه اولیه فاش می شوند و بخش اصلی آنها همچنان مخفی خواهند ماند و به احتمال زیاد رسیدن به محتوای بخش اول برای این افراد قانع کننده خواهد بود و آنها را از پیگیری بیشتر باز خواهد داشت. همچنین این بخش مخفی به هیچ وجه قابل ردیابی و تشخیص از طریق کنترل حجم فایل نیست. البته باید توجه داشته باشید که اگر مقدار فایلی بیش از گنجایش فضای

True Crypt درون آن بریزید، برنامه ممکن است فایل های بخش مخفی را از بین برده و فایل های شما را جایگزین آنها کند.

مراحل نصب و راه اندازی True Crypt

True Crypt یک نرم افزار رایگان است و بدون هیچ گونه پرداختی می توانید آنرا دانلود کنید.

- برنامه را اجرا کرده و بر روی Create Volume کلیک کنید.
- در صفحه ای که نمایش داده می شود گزینه ی Create an encrypted file container را انتخاب کنید، و سپس بر روی کلید Next کلیک کنید. توجه داشته باشید که دو گزینه دیگر تمام یک درایو انتخابی را فرمت کرده و آن را تبدیل به یک درایو حفاظت شده می کند.
- صفحه دیگری ظاهر می شود و مجددا گزینه ی اول (standard TrueCrypt volume) را انتخاب کنید و سپس بر روی Next کلیک کنید. با انتخاب این گزینه شما یک فضای محافظت شده یک لایه ساده خواهید داشت. اما اگر به دو فضای محافظتی مجزا با دو رمزعبور جداگانه در دل یکدیگر نیاز دارید، از گزینه دوم استفاده کنید.
- در مرحله ی بعد بر روی Select File کلیک کنید و یک فایل جدید بسازید. این فایل می تواند هر نام و پسوندی داشته باشد. توجه داشته باشید که برای امنیت بیشتر حتما گزینه ی never save history تیک خورده باشد. اگر از پسوندهای برنامه یا فایل های معمول ویندوز برای فایل تان استفاده کرده باشید، هنگام زدن دکمه ی Next با اخطاری مبنی بر اینکه ممکن است هم‌نامی با فایل های دیگر باعث مشکل شود، مواجه شوید. گزینه ی Yes را برای رفتن به مرحله ی بعد انتخاب کنید.
- در ادامه برای انتخاب سیستم کد گذاری از شما سوال می شود. پیشنهاد ما گزینه ی AES برای Encryption Algorithm و RIPEMD-160 برای Hash Algorithm است. حال دکمه Next را بزنید.
- در اینجا باید اندازه ی گاو صندوق خود را انتخاب کنید، دقت داشته باشید که این اندازه در آینده قابل تغییر نیست. پس به میزان فضایی که نیاز خواهید داشت و همچنین همخوانی آن با حجم معمول نوع فایل انتخابی توجه داشته باشید. با زدن کلید Next به پنجره بعدی بروید.

- حالا زمان انتخاب یک رمز عبور مطمئن است. رمزی که اگر آن را فراموش کنید به منزله از دست دادن کلیه اطلاعاتتان است. رمز عبور را با دقت و با رعایت اصولی که در درس اول مطالعه کرده اید انتخاب کنید.

- در صورتی که گزینه ی Use Keyfiles را انتخاب کنید، می توانید یک یا چند فایل جداگانه را به عنوان «کلید» گاو صندوق تان انتخاب کنید. این یعنی برای دسترسی به True Crypt نه تنها به رمز عبور نیاز خواهید داشت، بلکه باید فایل های انتخابی در این مرحله را داشته باشید. این کلیدها می توانند فایل های عکس یا آهنگ و غیره باشند. این کار مانند این است که یک گاو صندوق برای باز شدن، دو یا چند کلید همزمان بخواهد یا اینکه علاوه بر درخواست کد، اثر انگشت و تصویر قرنیه ی چشم را هم چک کند. اما توجه داشته باشید در صورتی که فایل مربوطه مفقود شده یا تغییر کند، شما برای همیشه اطلاعات درون True Crypt را از دست داده اید.

- در صفحه ی Volume Format گزینه FAT و Default را انتخاب کنید و Random Pool را تیک بزنید. در این مرحله برنامه برای تولید یک الگوریتم تصادفی و امن رمزگذاری، از شما می خواهد که مکان نمای موس را بر روی پنجره به حرکت درآورید. هر چه این حرکات تندتر و طولانی تر باشند، الگوریتم رمزگذاری شما قوی تر خواهد بود. مدت زمان ۳۰ ثانیه تا یک دقیقه برای این کار مناسب به نظر می رسد. هر وقت که فکر می کنید موس را به اندازه کافی حرکت داده اید، دکمه Format را بزنید تا فایل True Crypt شما ساخته شود. نکته: در صورتی که اندازه ی فایل انتخابی شما بیش از ۴ گیگابایت باشد، برنامه پیغام می دهد که شما نمی توانید از فرمت FAT استفاده کنید و تنها گزینه NTFS خواهد بود.

- اگر تا اینجا درست پیش رفته باشید، پیغامی با متن « The TrueCrypt Volume has been successfully created» را مشاهده می کنید.

تا اینجا شما یک گاو صندوق قابل اعتماد و با امنیت بالا دارید و سوالی که در اینجا مطرح می شود این است که چه طور از آن استفاده کنید و به صورت امن در آن را باز و بسته کنید؟

دسترسی به اطلاعات درون فایل True Crypt

- به صفحه ی اصلی برنامه برگردید. اینجا یکی از حروف الفبای موجود در لیست را انتخاب کنید.
- بر روی گزینه ی Select File کلیک کنید و فایل True Crypt را که قبلا ساخته اید، انتخاب کنید.
- بر روی Mount کلیک کنید و رمز عبور خود را وارد کنید (اگر فایلی را به عنوان کلید معرفی کرده اید، آن را هم انتخاب کنید).
- حالا می بینید کنار حرفی که انتخاب کرده بودید گاو صندوق تان اصطلاحا Mount شده است. کافی است به My Computer رفته و درایو جدیدی که ظاهر شده است را باز کنید.

الان می توانید فایل های مورد نظر خود را در این قسمت قرار دهید و بعد از تمام شدن کارتان، فایل ها را بسته و در صفحه ی اصلی برنامه بر روی Dismount All کلیک کنید تا گاو صندوق بسته شود. گاو صندوقی که ساختید را می توانید مثل یک فایل معمولی بر روی سی دی رایت کنید یا بر روی کول دیسک یا هر ابزار دیگری بریزید. حال فقط به برنامه True Crypt نیاز خواهید داشت که آن را باز کنید، که برای این منظور می توانید نسخه ی پرتابل اش را به همراه داشته باشید.

نکته ای که در اینجا وجود دارد و حتما باید آنرا در نظر بگیرید این است که گاو صندوقی که ساخته اید فایل های شما را مخفی و رمزنگاری می کند. اما هر کس که به کامپیوترتان دسترسی داشته باشد، می تواند آن را پاک کند و برای شما مشکلات اساسی ایجاد کند.

امنیت این روش برای نگهداری اطلاعات بسیار بالا است و اگر درست عمل کنید و رمز عبور پیچیده و طولانی داشته باشید، شکستن چنین دیواره دفاعی تقریبا غیرممکن است. اما همانطور که قبلا گفته شد، بهتر است که از نگهداری اطلاعات غیر ضروری خودداری کنید و در مواردی حتی مجبور به از بین بردن اطلاعات هستید.

پاک کردن اطلاعات به صورت امن

آیا تا امروز برای از بین بردن اطلاعات تان به پاک کردن آنها و خالی کردن سطل آشغال کامپیوتر بسنده می کردید؟ اگر این طور بوده، مرتکب اشتباه بزرگی شده اید. همان طوری که حتی بعد از پاک

کردن تخته سیاه اثر گچ بر روی آن باقی می ماند، آثار اطلاعات ذخیره شده هم بر روی هارد کامپیوتر باقی خواهند ماند و به وسیله ی هر فردی که ابزار مناسب را در اختیار داشته باشد و کمی هم خوش اقبال باشد قابل بازیابی است.

از بین بردن اطلاعات بهترین راه حفاظت از آنها است، البته اگر این کار به شکل صحیح و با رعایت اصول انجام نشود، عواقب ناگواری را به همراه خواهد داشت.

نرم افزارهایی مانند Eraser اطلاعات شما را به صورت کامل و برای همیشه از بین می برند. تفاوت استفاده از این نرم افزارها با حالتی که شما به صورت معمولی اطلاعات را پاک می کنید، مانند این است که کاغذی را مچاله کرده و درون سطل آشغال بیاندازید و آنگاه امیدوار باشید که کسی آن را پیدا نمی کند یا اینکه کاغذ را با کاغذ خردکن نابود کنید.

اگر از این زاویه به اطراف خود نگاه کنید که همواره افرادی با اهداف خصمانه اطلاعات شما را دنبال می کنند تا از اسرار حرفه ای و شخصی شما مطلع شوند، اهمیت نابودی صحیح و مطمئن اطلاعات برای شما روشن تر می شود. آیا می دانید که هنگام دور انداختن هارد قدیمی تان و یا سی دی های اطلاعات قدیمی چه باید کرد؟ یا اینکه چگونه مراقب باشیم تا فایل های Temp و موقتی سیستم عامل و برنامه ها دردسرساز نشوند؟

نکته فنی که شاید تاکنون از آن بی اطلاع بوده اید، این است که در واقع عملکردی به نام پاک کردن در کامپیوتر وجود ندارد. البته شما به راحتی یک فایل را به سطل آشغال ویندوز منتقل می کنید و سپس آن را نیز به طور کامل خالی می کنید و فضای اشغال شده ظاهرا آزاد می شود، اما در حقیقت شما تنها اسم فایل را حذف کرده اید و به ویندوز اجازه داده اید که از این فضا برای نگهداری اطلاعات دیگری استفاده کند. تا زمانی که فضای مذکور به وسیله ی فایل دیگری اشغال نشود، اطلاعات آن همچنان بر روی هارد دیسک پا بر جا است. بنابراین اگر نرم افزار مناسبی داشته باشید و به اندازه ی کافی سریع عمل کنید، می توانید اطلاعات از دست رفته خود را که اشتباها پاک کرده اید، دوباره به دست آورید.

همواره به خاطر داشته باشید که هر گاه از کامپیوترتان استفاده می کنید، اطلاعات زیادی بدون آگاهی و کنترل شما بر روی هارد دیسک ذخیره و حذف می شوند. به عنوان مثال زمانی که یک هفته

کاری تان صرف نوشتن یک مقاله یا گزارش اداری می شود، هر روز چندین ساعت را صرف نوشتن می کنید و هر بار که تغییرات جدیدی را بر روی آن اعمال می کنید، یک نسخه ی جدید از فایل بر روی سیستم ایجاد می شود که کاملا مجزا از نسخه ی قبل نگهداری می شود. البته ویندوز تنها آخرین فایل را به عنوان نسخه ی نهایی به شما نمایش می دهد، اما بقیه نسخه ها نیز تا زمانی که فضای اشغال شده توسط آنها مورد نیاز نباشد، همچنان بر روی سیستم باقی می مانند. به همین دلیل در صورتی که شما بخواهید این مقاله را از بین ببرید، پاک کردن آخرین نسخه اصلا کافی نیست.

دقت داشته باشید که سایر حافظه های موجود از جمله CDها، DVDها، USBها و حافظه های جانبی دوربین ها نیز از این قواعد مستثنی نیستند و قوانین ذخیره فایل ها برای آنها نیز همین گونه است.

پاک سازی اطلاعات با ابزار امن

هنگامی که برای حذف اطلاعات از ابزار مناسبی استفاده کنید، احتمال بازیابی آنها را تا حد زیادی کاهش می دهید. اگر اطلاعات هارد دیسک را به پرونده های درون کمد اسناد تشبیه کنیم، نرم افزار Eraser نه تنها این اطلاعات را پاک می کند، بلکه همان طور که با خودکار نوشته ها را خط زده و غیر قابل خواندن می کند، با نوشتن اطلاعات به درد نخور و پاک کردن مکرر، احتمال بازیابی آنها را کم می کند. Eraser این فرآیند را چندین بار تکرار می کند و با هر بار تکرار، بازیابی اطلاعات اولیه را سخت تر می کند. کارشناسان معتقدند که این عمل باید سه بار یا بیشتر تکرار شود اما استانداردهای قوی تر ۳۵ بار را توصیه می کنند. البته این امکان را هم دارید تا تعداد دفعات این کار را خودتان تعیین کنید.

پاک سازی فایل ها

پاک سازی اطلاعات از روی حافظه معمولا به دو شکل انجام می شود. شما می توانید تنها یک فایل را پاک سازی کنید و یا این فرآیند را بر روی تمام فضای آزاد حافظه انجام دهید.

نسخه های متعددی از یک گزارش بلند بر روی هارد دیسک شما در هر بار ذخیره ی فایل به وجود آمده و تنها نسخه ی نهایی آن قابل دسترس است. زمانی که شما نسخه ی نهایی فایل را پاک سازی می کنید، می توانید یقین داشته باشید که کامل ترین نسخه را از بین برده اید، اما همچنان فایل های زیادی از گزارش بر روی حافظه باقی مانده است. در واقع راه مستقیمی برای از بین بردن این

فایل ها وجود ندارد، زیرا آنها قابل رویت نیستند. در صورتی که عملیات پاک سازی را بر روی فضاهای خالی حافظه انجام دهید، کلیه ی نسخه های ذخیره شده از بین خواهند رفت.

Eraser یک نرم افزار ایمن، رایگان و متن باز است که به سادگی می توانید از آن برای پاک سازی اطلاعات خود استفاده کنید. این نرم افزار پاک سازی اطلاعات را به سه روش پاک سازی یک فایل مشخص، پاک سازی سطل آشغال و پاک سازی تمام فضاهای خالی حافظه انجام می دهد. همچنین می تواند فایل های ساخته شده توسط سیستم عامل را (Swap File) از بین ببرد.

البته همواره قبل از پاک سازی اطلاعات دقت کنید که نسخه ی پشتیبان مناسبی از اطلاعات ضروری تان تهیه کرده باشید. Eraser را می‌توانید از اینجا دانلود کنید.

پاک سازی فایل های موقت (Temporary)

در زمانی که از ویژگی پاک سازی فضاهای خالی حافظه در Eraser استفاده می کنید، هیچ خطری سایر اطلاعات شما را تهدید نمی کند، زیرا نرم افزار هیچ تاثیری بر روی اطلاعات ذخیره شده و قابل رویت شما نمی گذارد. این برنامه فقط فایل هایی را که قبلا پاک کرده اید را از بین می برد و به فایل های مهم و حساسی که به شکل مناسبی حفاظت می شوند و مخفی شان کرده اید، کاری ندارد.

اما در این بین فایل هایی وجود دارند که حاوی اطلاعات مهمی هستند. فایل هایی که زمان کار با کامپیوتر به صورت خودکار به وجود می آیند و شما از وجود آنها بی اطلاع هستید. فایل هایی مانند:

- فایل های ذخیره شده توسط مرورگر در زمان نمایش وب سایت ها که شامل متن، عکس، کوکی ها و اطلاعات کاربردی و شخصی شما هستند.
- فایل های موقت ذخیره شده توسط برنامه های کاربردی مانند Word که با هدف برگرداندن اطلاعات در صورت از کار افتادن سیستم قبل از ذخیره فایل، ایجاد می شوند. این فایل ها می توانند شامل متن، عکس و... باشند.
- فایل ها و لینک هایی که برای سادگی کار شما به وسیله ی ویندوز به وجود می آیند. مانند میانبرهایی که برای برنامه های مختلف ایجاد می شوند و یا محتوای سطل آشغال که فراموش کرده اید آن را خالی کنید.

- فایل های Swap ویندوز. هنگامی که حافظه ی کامپیوتر (RAM) شما پر می شود، مثلا زمانی که چندین برنامه را هم زمان اجرا می کنید، ویندوز اطلاعات را درون یک فایل نسبتا بزرگ ذخیره می کند که اصطلاحا Swap نامیده می شود. این فایل می تواند حاوی اطلاعات مهمی از قبیل عکس، متن، رمز عبور و خیلی موارد دیگر باشد. ضمنا زمانی که شما کامپیوتر را خاموش می کنید، این فایل ها از بین نمی روند و تا زمانی که آنها را پاک نکنید بر روی سیستم باقی خواهند ماند.

برای پاک کردن فایل های موقت (Temporary) از روی کامپیوتر می توانید از نرم افزار رایگان CCleaner استفاده کنید. استفاده از CCleaner بعد از هر بار استفاده از نرم افزارهایی همچون Microsoft Office و یا مرورگرهای مختلف و نرم افزارهایی از این دست که امکان بر جا گذاشتن اطلاعات مهم توسط آنها زیاد است، ضروری به نظر می رسد. این نرم افزار تنظیماتی دارد که می تواند حذف اینگونه اطلاعات را به صورت امن انجام بدهد. می توانید CCleaner را از اینجا دانلود کنید.

نکاتی برای استفاده صحیح از نرم افزارهای پاک سازی

تا اینجا با مواردی که اطلاعات شما پس از پاک شدن همچنان در دسترس دیگران قرار دارند، آشنا شدید و نرم افزارهای مناسب برای پاک سازی اطلاعات را نیز شناختید. اکنون به ذکر نکاتی می پردازیم که رعایت آنها برای کار بهتر با این نرم افزارها ضروری است.

- قبل از هر کاری یک نسخه پشتیبان رمزنگاری شده از اطلاعات خود تهیه کنید.
- تمامی برنامه های غیر ضروری را بسته و اینترنت را هم قطع کنید.
- کلیه فایل های به درد نخور و اضافی را از روی حافظه های مختلف پاک کنید و سطل آشغال را هم خالی کنید.
- با استفاده از CCleaner فایل های موقت (Temporary) ایجاد شده را پاک کنید.
- با استفاده از Eraser فایل های Swap ویندوز را پاک کنید.
- کلیه ی فضاهای خالی حافظه کامپیوتر را با استفاده از Eraser پاک سازی کنید. این مرحله را در زمان مناسبی مثلا در طول شب انجام دهید، زیرا زمان بر است.

کارهایی که باید به صورت مستمر و دوره ای انجام شوند عبارتند از:

- با استفاده از CCleaner فایل های موقت را از روی سیستم پاک کنید.
- برای پاک کردن فایل ها به جای استفاده از ابزارهای ویندوز و سطل آشغال از Eraser استفاده کنید.
- در بازه های زمانی مشخص فایل های Swap ویندوز را به وسیله Eraser پاک کنید.
- پاک سازی فضاهای خالی حافظه را از یاد نبرید، زیرا اطلاعات بسیاری به صورت پنهان در آنجا باقی می مانند.

نکاتی برای پاک سازی محتوای ابزارهای مختلف ذخیره سازی

در شرایطی ممکن است که بخواهید تمامی محتوای هارد دیسک و یا حافظه ی دیگری را از بین ببرید. به عنوان مثال زمانی که قصد دارید که کامپیوتر خود را بفروشید و یا وقتی که هارد دیسک جدیدی خریده اید و قصد دور انداختن هارد قدیمی را دارید. البته در مواردی که قصد فروش کامپیوتر را دارید، بهتر است که هارد دیسک را جدا کرده و از خریدار بخواهید برای خودش یک هارد دیسک تازه تهیه کند. در مواردی هم که قصد دور انداختن یک حافظه را دارید، بهتر است علاوه بر پاک سازی اطلاعات، به صورت فیزیکی هم آن را تخریب کنید.

در هر یک از موارد بالا و یا هر مورد مشابهی که پاک سازی کل حافظه ضرورت پیدا می کند، باز هم Eraser بهترین گزینه است. با این تفاوت که برای پاک سازی کامل هارد دیسک باید آن را از کامپیوتر جدا کرده و به صورت یک درایو جانبی به کامپیوتر دیگری متصل کنید. در شرایطی که فایل های سیستم عامل بر روی یک درایو قرار داشته باشند و درایو به صورت فعال توسط کامپیوتر در حال استفاده باشد، پاک سازی کلی آن امکان ندارد، زیرا Eraser تنها فضاهای خالی حافظه را پاک سازی می کند.

اگر قصد نابود کردن اطلاعات ذخیره شده بر روی CD و یا DVDهای Rewritable را دارید، بهترین راه نابود کردن آنها به صورتی فیزیکی است و اگر به بخشی از اطلاعات آنها نیاز دارید، قبل از تخریب این اطلاعات را بر روی یک حافظه دیگر ذخیره کنید. برای انواع معمولی هم که راه دیگری غیر از تخریب فیزیکی وجود ندارد. شاید شما در مورد بازیابی اطلاعات از سی دی ها و دی وی دی ها حتی پس از

تبدیل شدن آنها به تکه های ریز چیزهایی شنیده باشید. البته بازیابی اطلاعات ذخیره شده بر روی این نوع از حافظه ها بسیار سخت است و این به شما بستگی دارد که فکر می کنید اسرار شما تا چه حد برای دیگران مهم خواهد بود، زیرا بازیابی این اطلاعات تنها با صرف وقت و هزینه زیاد مقدور است. اگر از افشای اطلاعات تان واهمه دارید، می توانید پس از تخریب سی دی یا دی وی دی، تکه های آن را در محل های مختلفی دور از محیط کار و زندگی خود پراکنده کنید.

اینکه اطلاعات شما تا چه حد برای سایرین مهم است و افراد حاضر به صرف وقت و انرژی برای دستیابی به آنها هستند، قطعا در زمان ها و موقعیت های مختلف متفاوت است و شما می توانید با همین تناسب برای نابودی اطلاعات تان وسواس به خرج دهید. اما شکی نیست که رعایت اصول امنیت برای تمام افراد ضرورت دارد.

درس یازدهم – مدیریت رمزهای عبور

همانطور که در درس اول دیدیم، هر زمان که در مورد رمزعبور صحبت می شود، گفته می شود رمزعبور انتخابی باید سخت و پیچیده بوده و برای هر سایتی متفاوت از دیگری باشد. اما به راحتی می شود فهمید که انجام چنین کاری بسیار مشکل است و به خاطر سپردن چنین رمزهای عبوری تقریبا غیر ممکن است. به همین جهت ابزارهای زیادی جهت نگه داری امن رمز عبور تولید شده است، به این نرم افزارها Password Manager می گویند که کارشان نگهداری رمز عبور به همراه نام کاربری تان است. اغلب آنها به هر سایتی که مراجعه می کنید به صورت خودکار نام کاربری و رمز عبورتان را وارد می کنند تا هم از دست تایپ کردن آنها راحت باشید و هم از دست به خاطر سپردن شان.

روی اغلب مرورگرها هم این امکان به صورت پیش فرض وجود دارد. حتما تا به حال هنگام ورود به ایمیل تان با پیام مرورگرتان مواجه شده اید که آیا می خواهید نام کاربری و رمز عبورتان برای این سایت به خاطر سپرده شود یا خیر؟

پس چرا با وجود در دسترس بودن این نرم افزارها یک درس از این دوره را به آنها اختصاص داده ایم؟ تمام پاسخ در مورد تفاوت های امنیتی و کاربردی این نرم افزارها است. همانطور که گفتیم نسخه های رایگان و پولی متفاوتی از این نرم افزارها وجود دارد، آنها امکانات مختلفی ارایه می کنند و مهم تر از آن امنیت شان با یکدیگر متفاوت است.

شما به نرم افزار مدیریت پسوردی نیاز دارید که در عین داشتن امکانات خوب، امنیت بالا و قابل اعتمادی داشته باشد. چرا که قرار است تمام رمزهای عبورتان را به دستش بدهید و در صورت بروز مشکل، تقریبا همه چیز را از دست خواهید داد. برای مثال مرورگر فایرفاکس چنین امکانی را در اختیارتان قرار می دهد، اما اگر فرد دیگری به کامپیوتر شما دسترسی داشته باشد این امکان را دارد که تمام رمزهای عبورتان را ببیند. بنابراین باید آن را از لیست تان برای انجام چنین کاری حذف کنید.

در اینجا به جای معرفی چند نرم افزار مختلف ترجیح دادیم یکی از بهترین و خوش دست ترین آنها را معرفی کنیم.

شاید شما از نرم افزارهای مدیریت پسورد زیادی استفاده کرده باشید و در حال حاضر هم مشغول استفاده از یکی از آنها باشید، در این درس قصد داریم LastPass را به شما معرفی کنیم. این نرم افزار در واقع افزونه ای تقریبا رایگان است که بر روی اکثر مرورگرها و همچنین در حالت پولی بر روی تلفن های هوشمند نصب می شود و با سازگاری ای که با نرم افزار KeePass دارد، کار را برای افرادی که به طور همزمان از KeePass هم استفاده می کنند، راحت می کند.

چرا LastPass؟

زمانی که صحبت از مرورگرها و رمزهای عبور وب سایت ها به میان می آید، LastPass می تواند قابلیت های خود را نشان دهد و یک سر و گردن بالاتر از رقیب های خود بایستد. در اینجا تعدادی از مزیت های LastPass را برای شما برمی شماریم:

- **عمومیت LastPass:** افزونه هایش را تقریبا برای همه مرورگرها و در همه ی سیستم های عامل در اختیار کاربران قرار داده است. فایرفاکس، اینترنت اکسپلورر، کروم و سافاری در ویندوز، مک و لینوکس، امکان استفاده از افزونه ی LastPass را دارند.
- **سادگی LastPass:** انتخاب ها، تنظیمات و ابزارهای زیادی در هنگام کار برای کاربر فراهم می کند. اگر شما می خواهید از میان بهترین نرم افزارهای مدیریت رمز عبور، یکی را انتخاب کنید که نصب و استفاده از آن امن و ساده باشد و به سرعت لاگین شود، LastPass انتخاب مناسبی خواهد بود. برای مثال این نرم افزار در هنگام کار به صورت خودکار از شما می خواهد رمز عبورها و فرم هایی که پر کرده اید ذخیره کنید؛ البته شما می توانید این قابلیت را خاموش کنید.
- **امنیت:** هنگام استفاده از این نرم افزار احتمال از بین رفتن رمزهای عبورتان بسیار کم می شود، چرا که بانک اطلاعات پسوردهای شما به جز هاردتان، بر روی سرورهای امن LastPass هم ذخیره می شود.

  البته ذخیره شدن رمزهای عبور بر روی سرورهای LastPass ممکن است این نگرانی را به وجود آورد که در صورت هک شدن این سرورها، اطلاعات حیاتی کاربران در اختیار هکرها قرار بگیرد و یا اینکه وب مسترهای این شرکت امکان سوء استفاده از این اطلاعات را داشته باشند.

LastPass این نگرانی را هم با استفاده از سیستم میزبانی host-proof برطرف کرده است. در این سیستم اطلاعات شما به صورت متن عادی نگه داری نمی شوند، بلکه در کامپیوتر شما به صورت بسته های رمزگذاری شده کاملا امنی درآمده و برای سرور ارسال می شوند. در این حالت کلید باز کردن این رمزگذاری تنها بر روی کامپیوتر شما و در اختیار شما است و اطلاعات بر روی سرور به هیچ وجه قابل خوانش نیستند. هنگامی که از رمزهای عبور ذخیره شده استفاده می کنید، رمزگشایی اطلاعات به جای سرور بر روی کامپیوتر خودتان انجام می شود.

اگر شما در حال استفاده از یک برنامه ی مدیریت رمز عبور هستید، مهاجرت به LastPass بسیار ساده است. چرا که LastPass می تواند رمزهای عبور استخراج شده از اکثر نرم افزارها و سایت های مدیریت رمز عبور را دریافت کند.

روش استفاده از LastPass

برای استفاده از این نرم افزار ابتدا باید از طریق این آدرس، یک حساب کاربری در سایت LastPass ایجاد کنید تا پس از دانلود و نصب افزونه برای مرورگرهای مورد نظر خود بتوانید در LastPass وارد شوید. البته شما می توانید ثبت نام را هنگامی که افزونه را بر روی یکی از مرورگرهای خود نصب کردید هم انجام دهید. عملیات ثبت نام را با دقت انجام دهید و اصول انتخاب رمزعبور مناسب را در انتخاب رمز اصلی خود در LastPass به کار گیرید.

هنگام ثبت نام در سایت LastPass شما باید یک رمز عبور اصلی برای دسترسی به نرم افزار انتخاب کنید. این رمز در واقع مانند یک شاه کلید عمل می کند تا از طریق آن به بقیه ی رمزهای عبورتان دسترسی داشته باشید. بنابراین طبیعی است که باید این رمز را بسیار با دقت و پیچیده انتخاب کنید. با روش های خوب انتخاب رمز عبور مناسب در درس های قبلی این دوره آشنا شده اید. اگر نیاز است آنها را یک بار مرور کنید.

البته همانطور که می دانید لازم است فقط همین یک رمز را به خاطر بسپارید و کار حفظ کردن بقیه رمزهای عبور بر عهده ی نرم افزار LastPass است.

هشدار: دقت کنید که رمز عبور اصلی نرم افزار را هیچ گاه فراموش نکنید. در صورت فراموش کردن آن راه های بسیار محدودی برای بازگرداندن اکانت و دسترسی به پسوردها وجود دارد. برای اطلاعات بیشتر در این مورد می توانید این صفحه را بخوانید.

اولین باری که افزونه LastPass را در مرورگر خود نصب می کنید، با کلیک بر روی کلید LastPass که در گوشه ی مرورگر ظاهر می شود. اگر بر روی آن کلیک کنید، منویی باز می شود که اطلاعات و انتخاب های زیادی را به شما می دهد.

نکته امنیتی: در هنگام لاگین در افزونه ی LastPass، دقت کنید که تیک گزینه ی remember that password را بردارید.

از این به بعد، اگر شما در سایتی لاگین کنید، LastPass در یک منوی پایین افتادنی (Drop down) از شما سوال می کند که آیا می خواهید نام کاربری و رمز عبور این سایت در بانک اطلاعاتی LastPass ذخیره شود یا خیر.

همچنین هنگام ثبت نام در سایت های جدید، هنگام پر کردن کادر رمز عبور، LastPass می تواند به شما در انتخاب یک رمزعبور مناسب و امن با تعداد و نوع کارکترهای دلخواه، کمک کند. توصیه می شود که از این قابلیت استفاده کنید تا از رمزهای عبور تصادفی و قدرتمندی که LastPass پیشنهاد می دهد نهایت استفاده را ببرید. چرا که دیگر نگران به خاطر آوردن و فراموش کردن آنها نخواهید بود.

چند تنظیم مفید و مهم

بعد از ثبت نام و نصب افزونه بر روی مرورگر بهتر است بر روی آیکون LastPass کلیک کنید و گزینه ی Preferences را انتخاب کنید. در آنجا بر روی Account Settings کلیک کنید و به قسمت Security بروید. بهتر است که تنظیمات این قسمت را مطابق تصویر پایین تغییر دهید تا امنیت بیشتری داشته باشید. البته می توانید مطابق میل‌تان آنها را تنظیم کنید.

در این صفحه گزینه ای وجود دارد به نام Grid Multifactor Authentication؛ اگر رمزهای عبورتان برای شما بسیار مهم است و به دنبال امنیت مضاعف هستید، می توانید از این گزینه استفاده کنید. با این کار LastPass یک جدول اعداد و حروف در اختیارتان قرار می دهد که باید آن را چاپ کنید. برای

هر بار لاگین کردن به اکانت علاوه بر ایمیل و رمز عبور اصلی باید تعدادی از حروف این جدول را هم وارد کنید که سایت از شما درخواست قسمت های خاصی از آن را می کند. این کار برای این است که هیچ کس نتواند از کامپیوترهای دیگر به اکانت شما وارد شود. ضمنا می توانید بعد از یک بار ورود از این طریق، کامپیوتر خودتان را به عنوان کامپیوتر مورد اعتماد معرفی کنید تا دیگر برای لاگین از طریق این کامپیوتر رمز جدولی خواسته نشود. البته استفاده از این امکان را فقط برای کاربران حرفه ای تر و دقیق توصیه می کنیم.

One-Time Passwords یا رمزعبورهای یکبار مصرف

گاهی اوقات پیش می آید که در یک مکان یا شبکه بی سیم نه چندان امن، نیاز به استفاده از LastPass خود داشته باشید. باید بدانید در صورتی که نام کاربری و رمزعبور اصلی خود را در آن کامپیوتر یا شبکه وارد کنید، این احتمال وجود دارد که رمزعبور خود را تقدیم صاحب سیستم یا مدیر شبکه مذکور نمایید. راه حلی که LastPass پیشنهاد می کند، استفاده از یک رمزعبور یکبار مصرف است.

برای این کار ابتدا بر روی یک کامپیوتر و شبکه امن در مرورگر خود وارد سایت LastPass شده و با مشخصات کاربریتان در آن لاگین کنید. می توانید با مراجعه به صفحه ی تولید رمزعبور یکبار مصرف، با استفاده از دکمه ی Add a new One Time Password به هر تعداد که نیاز داشته باشید رمزعبور یکبار مصرف بسازید یا آن ها را مدیریت کنید. حال می توانید این رمزعبورها را چاپ کرده یا حفظ کنید و با خود همراه داشته باشید، تا در آینده هر کجا که به رمزهای عبور خود نیاز داشتید با مراجعه به این صفحه ایمیل خود را وارد کرده و به جای رمز عبور اصلی LastPass، یکی از این رمزعبورهای یکبار مصرف را مورد استفاده قرار داده و به تمامی اطلاعات ذخیره شده دسترسی داشته باشید. اگر آنها را چاپ کردید، کاملا مراقب باشید که در جای امنی باشند و آنها را گم نکنید.

نکته جالب اینجاست که به محض ورود به سایت با یک رمزعبور یکبار مصرف، آن رمزعبور باطل شده و به هیچ وجه قابل استفاده نیست، پس حتی اگر کسی بعد از لاگین به آن دست یابد، خطری برای شما نخواهد داشت. در صورتی هم که از اطلاعات کاربری داخل LastPassتان به صورت کپی و

پیست استفاده کنید، به احتمال زیاد از خطر سرقت اطلاعات توسط بدافزارهایی از قبیل کی‌لاگرها در امان خواهید بود

Secure Notes یا یادداشت های امن

اگر شما به دنبال محلی برای ذخیره ی نوشته های مهمی از قبیل PIN کارت بانک و یا سوال امنیتی ایمیل و پاسخ آن هستید، یادداشت های امن LastPass کمک بزرگی به شما می کنند. چرا که این یادداشت ها همانند رمزهای عبور شما به صورت کاملا امن و رمزگذاری شده نگهداری می گردند. یک مثال خوب از کاربرد یادداشت های امن نگه داری پسورد شبکه ی بی سیم است که در درس بعدی با آن آشنا می شوید.

برنامه ی ویژه ی تلفن های همراه هوشمند

صفحه نمایش های کوچک، کلیدهای کوچک و فیلدهای ورود کوچک- به عنوان یک واقعیت آزاردهنده- در همه ی تلفن های هوشمند بطور یکسان وجود دارند. حتی اگر تلفن هوشمند شما قابلیت ذخیره ی امن رمزهای عبور را داشته باشد، همگام سازی (synchronize) آن با کامپیوتر کار راحتی نیست و این مورد مشکلاتی را به وجود می آورد.

اگر شما از تلفن های هوشمند سیمبیان، ویندوز موبایل، بلک بری، آندروید، آی فون و حتی پالم استفاده می کنید، می توانید نسخه ای از LastPass را دانلود کرده و از این نرم افزار در گوشی خود نیز بهره ببرید. البته نسخه های موبایلی LastPass همانند افزونه های قابل نصب بر روی مرورگرها، رایگان نیستند و بنابراین برای این حالت مجبور به پرداخت پول خواهید بود.

بدین ترتیب به راحتی با لاگین کردن در نرم افزار LastPass از طریق گوشی موبایل به رمزهای عبورتان دسترسی خواهید داشت.

نگهداری و استفاده از رمزهای عبور، از اصول پایه ای امنیت هستند و استفاده از ابزارهایی همانند LastPass علاوه بر افزایش ضریب امنیت رمزهای عبور شما، استفاده مکرر از آنها را برای شما آسان می نماید. بنابراین نرم افزارهای مدیریت پسوردها را فراموش نکنید.

درس دوازدهم – امنیت در شبکه های بی سیم

فراگیر شدن شبکه های بی سیم سبب شده که از دست سیم ها تا حدی راحت بشویم. اما وقتی از طریق یک کابل به شبکه یا اینترنت متصل هستید، حداقل خیال‌تان راحت است که کسی اطلاعات را در مسیر منتقله از کابل تا کامپیوتری که به آن متصل هستید، نمی بیند.

اما در یک شبکه ی بی سیم هر کسی که در برد امواج باشد، قادر است تا در ارتباط شما سرک بکشد و اگر اصول امنیتی لازم را رعایت نکرده باشید، به راحتی به اطلاعات شما دسترسی پیدا می کند. احتمالا در خانه یک شبکه ی بی سیم برای اشتراک اینترنت راه اندازی کرده اید یا اینکه قصد دارید در آینده یکی راه اندازی کنید. برای امن کردن آن چه کارهایی انجام می دهید؟ پاسخ این سوال و برخی موارد مهم دیگر را در این درس می خوانید.

شبکه های بی سیم توسط مودم یا اکسس پوینت و یا روتر بی سیم کار می کنند. بیشتر تنظیمات امنیتی باید در این دستگاه ها انجام شود. متاسفانه اکثر افراد تنظیمات اکسس پوینت را به حال پیش فرض خود رها می کنند و با این کار بزرگترین خطر را متوجه شبکه و اینترنت شان می کنند. اغلب از کاربران شبکه بی سیم می شنویم: «ای بابا تو همسایه های ما کی دیگه بلده وایرلس چیه؟ چه برسه به اینکه بخواد کاری هم بکنه!».

به نظر می رسد این افراد تا وقتی که پهنای باند گم نکنند، دسترسی به مودم شان را از دست ندهند یا از آن بدتر فایل های مهم را از دست ندهند، این داستان را جدی نمی گیرند. بهتر است بدانید داشتن شبکه ای امن و مطمئن کار چندان سختی نیست و بیش از ۱۵ دقیقه وقت نمی برد.

- در اولین قدم باید آدرسIP مودم یا روترتان را بیابید. این آدرس معمولا بر روی جعبه ی مودم بی سیم و یا صفحات اول دفترچه راهنمای آن نوشته شده است. برای مثال ممکن است آدرس آی پی مودم شما ۱۹۲٫۱۶۸٫۰٫۵۰ باشد. اگر این دو مورد کمکی به شما برای یافتن IP تان نکرد، می توانید از طریق خط فرمان سیستم و تایپ یک خط دستور، آن را پیدا کنید.
- برای ورود به صفحه ی خط فرمان (Command Prompt) در ویندوز XP این مسیر را دنبال کنید:

Command Prompt < Accessories < Programs < Start

البته راه نزدیک تر برای رسیدن به این بخش، استفاده از گزینه ی Run در منوی Start است و شما با تایپ دستور cmd وارد صفحه ی خط فرمان می شوید.

cmd < Run < Start

در ویندوز ویستا و ۷ هم می توانید با تایپ این عبارت در قسمت Search به صفحه ی خط فرمان وارد شوید.

cmd < Search < Start

در صفحه خط فرمان (که به رنگ مشکی و محیطی کاملا شبیه سیستم عامل داس است) تنها کافی است که دستور ipconfig/all را تایپ کرده و کلید Enter را بزنید. با این کار کلیه ی جزئیات مربوط به IP سیستم تان به نمایش در می آید. ممکن است لیستی بلند بالا و گیج کننده برایتان باز شود؛ نگران نشوید! این دستور در واقع آدرس آی پی و مشخصات تمام کارت های شبکه واقعی و مجازی کامپیوتر را به همراه مقدار دیگری اطلاعات نشان می دهد. در این لیست شما به دنبال مشخصات کارت شبکه بی سیم کامپیوتر هستید، بنابراین دنبال بخشی بگردید که نامی شبیه این داشته باشد: Ethernet adapter Wireless Network Connection. وقتی آن را پیدا کردید به دنبال عبارت Default Gateway در آن قسمت بگردید، معمولا عبارت نمایش داده شده در برابر آن همان IP مودم شما است.

- با پیدا کردن آدرس IP، قسمت سخت ماجرا را پشت سر گذاشته اید. حالا کافی است که این آدرس را در مرورگرتان وارد کرده و کلید Enter را بزنید تا به صفحه ی تنظیمات مودم یا روترتان وارد شوید. البته در این مرحله بسته به نوع مودم ممکن است از شما رمز عبور و نام کاربری خواسته شود که در دفترچه ی راهنمای آن نوشته شده است. اگر مودم شما توسط فرد دیگری تنظیم شده است، هنگام نصب اولیه ی مودم فراموش نکنید که نام کاربری و رمز عبور مودمتان را از نصاب بپرسید. چون ممکن است که وی رمز مودم را عوض کرده باشد. پس از گذراندن این مراحل وارد صفحه ای می شوید که از آنجا به تمامی تنظیمات شبکه بیسیم تان دسترسی دارید. البته شکل ظاهری این صفحه در مدل های مختلف مودم و روتر بسیار متفاوت است و ممکن است کمی شما را به دردسر بیاندازد.

- اولین دیوار دفاعی که باید در برابر بیگانگان ایجاد کنید، تغییر نام کاربری و رمز عبور صفحه ورود به تنظیمات مودم است، زیرا در صورتی که فردی بتواند وارد این قسمت شود، به تمام تنظیمات امنیتی شبکه تان دسترسی خواهد داشت. در بخش تنظیمات به دنبال دکمه ای با نام Administration یا Administrator Setting یا چیزی شبیه این باشید. در اینجا می توانید رمز عبور را تغییر دهید و حتی در برخی از مودم ها و روترها نام کاربری را هم تغییر دهید و یا از یکی دیگر از نام های کاربری موجود در تنظیمات به جای کلمه ی admin استفاده کنید.

- مودم یا روترتان معمولا توسط ابزارهایی که دارای قابلیت وای فای هستند، قابل جستجو است و در این جستجو نام کارخانه ی سازنده یا نام های عمومی از قبیل WLan نمایش داده می شود. یکی دیگر از دیواره های دفاعی قلعه شما تغییر این نام و استفاده از اسامی خاصی است که چندان معنا و جذابیتی برای فرد جستجوگر نداشته باشد و مشخص کننده ی نوع ارتباط یا جنس مودم تان نباشد. مثلا کلمه D-Link نشان دهنده این است که شما از یک مودم بی سیم د-لینک استفاده می کنید که هر فرد حرفه ای IP، نام کاربری و رمز عبور اولیه آن را می داند. استفاده از نام Ahmad's Network نشان دهنده ی این است که شما با یک شبکه اینترنت بی سیم شخصی سروکار دارید که ممکن است دارنده آن آشنایی چندانی با مسائل امنیت شبکه نداشته باشد، پس نفوذ به آن کار چندان سختی نباید باشد.

- یکی دیگر از قابلیت های مودم ها و روترهای بی سیم امکان رمز گذاری اطلاعات رد و بدل شده در شبکه است. بسته به نوع ابزار مورد استفاده، می توانید از سه روش رمز گذاری استفاده کنید که به ترتیب امنیت عبارت اند از:

الف- WPA2: اختصار کلمات Wi-Fi Protect Access 2 است و در حال حاضر امن ترین شیوه ی رمز گذاری اطلاعات در شبکه های بی سیم است که امروزه معمولا در بیشتر مودم های بی سیم و روترها یافت می شود. در صورتی که مودم یا روتر شما هم این گزینه را دارد، حتما حتما حتما از آن استفاده کنید.

ب- WPA: اختصار کلمات Wi-Fi Protected Access است و اگر سیستم رمز گذاری بالا را در مودم تان نیافتید، می توانید از این گزینه هم استفاده کنید که امنیت کمتر، اما قابل قبولی دارد.

ج- WEP: اختصار کلمات Wired Equivalent Privacy است و یکی از ناامن ترین سیستم های رمزنگاری است که باید مودم یا روترتان بسیار قدیمی باشد تا مجبور به استفاده از این گزینه باشید. اما به یاد داشته باشید که حتی این گزینه هم بسیار بهتر و امن تر از عدم استفاده از سیستم رمزگذاری است. اما باید بدانید که رمزنگاری در این روش به راحتی قابل شکستن است.

بسته به اینکه کدام یک از این سیستم های رمزگذاری را انتخاب کرده باشید، باید برای رمزنگاری اطلاعات تان رمز عبوری بین ۷ تا ۶۳ کاراکتر را انتخاب کنید. توصیه ما این است که حتما WPA2 با طولانی ترین رمز عبور ممکن یعنی ۶۳ کاراکتر را انتخاب کنید.

ممکن است بگویید حفظ کردن چنین پسوردی غیر ممکن است و تایپ آن هم کار سختی است. درست می گویید، اما نیاز نیست آن را حفظ کنید. می توانید آن را در یک فایل متنی و در جای امنی ذخیره کنید و با کپی/ پیست از آن استفاده کنید. ضمنا یک بار وارد کردنش در لپ تاپ کافی است و بعد از آن معمولا نیازی به وارد کردن مجدداش نیست.

این آدرس، پسوردهای قدرتمند و طولانی ای را برای شبکه ی بی سیم تان تولید می کند. بنابراین می توانید از آن کمک بگیرید.

- مک فیلتر (Mac Filter) را فعال کنید. هر قطعه سخت افزاری یک نام انحصاری مخصوص به خود دارد که «آدرس فیزیکی» نامیده می شود. برای مثال کارت شبکه ی بی سیم بر روی لپ تاپ، اکسس پوینت، تلفن های همراه و قطعات دیگر هر کدام آدرس فیزیکی خودشان را دارند که به آن مک آدرس هم می گویند. روی تمام اکسس پوینت ها امکانی به نام مک فیلتر وجود دارد که می توانید از طریق آن به مودم بگویید فقط به لپ تاپ ها و کامپیوترهای خاصی که از قبل تعریف شده اند اجازه ی ورود به شبکه را بدهد. دقت کنید این مرحله پیش از دریافت رمز عبور شبکه بی سیم اتفاق می افتد. بنابراین اگر این قابلیت را فعال کرده باشید، کامپیوترهای غریبه حتی اجازه رسیدن به مرحله ی وارد کردن رمز عبور را پیدا نمی کنند.

روشن کردن مک فیلتر مانند این است که خانه ی شما دو دروازه عبور داشته باشد. نگهبان جلوی درب اول، ابتدا از بازدیدکنندگان کارت شناسایی بخواهد، در صورتی که اسم آنها در لیست عبور باشد به آنها اجازه می دهد به در دوم برسند و در آنجا از آنها رمز عبور خواسته می

شود. با این روش امنیت شما خیلی بیشتر از قبل می شود. اما توجه کنید که این کار به هیچ عنوان سبب نمی شود که از یک رمز عبور قدرتمند بر مبنای WPA2 استفاده نکنید. چرا که جعل کارت شناسایی امکان پذیر است!
توصیه می شود که در شبکه های خانگی حتما این امکان را فعال کنید. کافی است که آدرس فیزیکی کامپیوترها و لپ تاپ های مجاز را به اکسس پوینت بدهید. برای این کار همان دستور ipconfig/all که در ابتدای این درس توضیح داده شد را در هر کدام از کامپیوترها اجرا کنید. در بخش مشخصات کارت شبکه ی بی سیم هر لپ تاپ می توانید در قسمتی به نام Physical Address، نام فیزیکی را پیدا کنید که معمولا به این شکل است: j:5g:8f:3p:pd۰۰:۳

- مکان اکسس پوینت را با دقت تعیین کنید. بهترین مکان در وسط خانه است. اگر اکسس پوینت در نزدیکی در خروجی و پنجره ها قرار بگیرد بیشتر از اینکه برای شما سیگنال دهی بکند برای همسایه ها و دیگران برای نفوذ مفید خواهد بود.

- در زمان سفر، شبکه ی بی سیم را خاموش کنید. هیچ دلیلی وجود ندارد وقتی برای مدتی طولانی به سفر می روید اکسس پوینت شبکه بی سیم را روشن بگذارید. با خاموش کردنش هم به بالا بردن امنیت خودتان کمک کرده اید و هم قبض برق کمتری خواهید داشت.

- آخرین مرحله هم مراقبت از نام کاربری و رمزهای عبوری است که برای امنیت بالاتر ساخته اید. توصیه نمی کنیم که آنها را در دفترچه راهنما یا جعبه ی مودم تان بنویسید. بهتر است در این مورد زیاد به حافظه اعتماد نکنید چون که فاصله استفاده مجدد از این تنظیمات طولانی است و تا آن موقع آنها را فراموش می کنید. بنابراین بهتر است آنها را در یک فایل رمزنگاری شده نگه داری کنید. البته فراموش کردن این اطلاعات تنها باعث زحمت دوباره ی تنظیم مودم خواهد شد، زیرا همه ی مودم و روترها در زیر خود کلیدی را برای ریست کردن دارند که باعث می شود تمام تنظیمات مودم به تنظیمات کارخانه ای برگردند. برای انجام این کار نیاز به سنجاق یا یک شیئ نازک دارید تا این کلید را بفشارید. فراموش نکنید که این کلید را حداقل ۱۰ تا ۱۵ ثانیه نگه دارید.

توجه: به خاطر داشته باشید که بعد از ریست کردن، حتما این تنظیمات امنیتی را دوباره انجام

دهید و ضمنا اگر از همان مودم برای اتصال به اینترنت مثلا ADSL استفاده می کنید، حتما تنظیمات اتصال به ADSL را از قبل جایی یادداشت کرده باشید چرا که با ریستارت کردن مودم همه ی این تنظیمات پاک می شود و باید از اول انجام بشود. کار سختی نیست، اما اگر آنها را نداشته باشید، برای تنظیم دوباره مجبور می شوید با شرکت ارایه دهنده ی خدمات اینترنتی خود تماس بگیرد و تنظیمات را از آنها سوال کنید.

درس سیزدهم – امنیت در شبکه های اجتماعی

امروزه دیگر گشت و گذار در وب، سفر یک نفره و مکاشفه در تنهایی نیست، زیرا شبکه های اجتماعی از قبیل فیس بوک، توییتر و... به بخش جدایی ناپذیری از فرهنگ زندگی آنلاین تبدیل شده اند. در کنار آن هر جا تعداد کاربر زیاد می شود، توجه ی هکرها و افراد سوء استفاده گر را هم به خود جلب می کند. برای همین، این شبکه ها در حال تبدیل شدن به حفره های مهم امنیتی هستند که هر روزه کاربران زیادی را در کام خود فرو می برند.

همانطور که همه روزه استفاده افراد از شبکه های اجتماعی از قبیل فیس بوک، توییتر و فرندفید بیشتر و بیشتر می شود، حفظ حریم خصوصی نیز اهمیت بیشتری پیدا می کند. عضویت در شبکه های اجتماعی همواره برای عده ی زیادی با نگرانی و اضطراب همراه بوده است و در مواردی نیز منجر به مشکلاتی هم شده است. کم نیستند افرادی که از برچسب خوردن عکس هایشان توسط دیگران و یا دیده شدن عکس های خصوصیشان توسط دوستان نه چندان صمیمی‌شان شاکی اند. در برخی جوامع این مشکل به اندازه ای زیاد شده که کلماتی مانند Facebook Fired به فرهنگ لغات هم راه یافته اند.

Urban Dictionary در توضیح این عبارت می نویسد: اخراج شدن از کار به دلیل استفاده بیش از حد از فیس بوک در ساعات کاری- آسیب دیدن و اخراج شدن به دلیل برخی چیزهایی که در فیس بوک نوشته اید!

در این درس به طور خلاصه به برخی خطرات بالقوه ی شبکه های اجتماعی و به خصوص فیس بوک می پردازیم و راه کارهایی برای کاهش این خطرات و همچنین حذف کامل اکانت در آنها ارائه خواهیم کرد.

نکته: مدتی است که تعدادی شبکه‌ی اجتماعی فارسی زبان از قبیل کلوب راه اندازی شده اند، که با استقبال خوبی هم از طرف کاربران ایرانی مواجه شده اند. اما در خصوص این سایت ها ذکر این نکته ضروری است که صاحبان آنها طبق قوانین ایران موظف اند که در صورت درخواست مقامات قضایی، تمامی اطلاعات کاربران را در اختیار مراجع مربوطه قرار دهند. این اطلاعات شامل تمامی عکس ها، نوشته ها و حتی مشخصات تماس و آی پی فرد می‌شود.

مواظب باشید که چه چیزی را به اشتراک می گذارید

همیشه در زندگی آنلاین‌تان همانند زندگی واقعی حد و مرزی برای ارتباطات تان قائل شوید. قبل از آنکه متنی را توییت کنید یا چیزی را در فیس بوک منتشر کنید، کمی تامل کنید و ببینید آیا کسی از دیدن آن آزرده نخواهد شد و یا اینکه در آینده برایتان مشکلی ایجاد نمی کند؟ اگر رئیس تان آن را ببیند چه اتفاقی خواهد افتاد؟ اگر گروه تایید صلاحیت شما در شغل جدیدتان به آن سر بزنند چطور، عکس های میهمانی یا اردو دوستانه سال گذشته برایتان مشکل ساز نمی شوند؟ مطالبی که در خصوص همکاران، مسئولین و محیط کارتان می نویسید، دردسری ایجاد نمی کنند؟

به عنوان یک اصل، همیشه چیزی را منتشر کنید که کسی در آینده نتواند آن را دست مایه ی سوءاستفاده از شما قرار دهد.

دوستان و دوستانِ دوستان تان را بشناسید و به خاطر داشته باشید

حواس تان باشد که لیست دوستان تان شامل چه کسانی است. حتی مراقب دوستان دوستان تان باشید، ممکن است آنها هم برایتان مشکل ساز شوند. ممکن است شما تنها به دوستان تان اجازه ی دیدن پست ها و عکس های فیس بوک تان را داده باشید، اما وقتی که دوستی برای شما کامنت می گذارد و یا مطلب‌تان را لایک می زند، آنگاه دوستان او هم قادر به دیدن مطلب شما هستند. شما از رئیس تان شاکی هستید و به تمسخر وی در فیس بوک می پردازید. هیچ کدام از روسا و مسئولین در لیست دوستان تان نیستند و آن را نمی بینند. همکارتان هم که در لیست دوستان تان است آن را لایک می زند، از شانس بد شما، جناب رئیس در لیست دوستان دوست لایک زن است و از طریق همین لایک، مطلب شما را می بیند. حالا وقت آن است که خر بیاورید و باقالی بار کنید!

شما یکی از ایرادات و یا مسائل مهم محل کارتان را توییت می کنید. مطمئن هستید که جناب رئیس نمی تواند توییت شما را ببیند، اما از شانس بد یکی از دوستان آن را دوباره توییت (retweet) می کند. حالا آقای رئیس آن را می بیند و شما را مورد نوازش قرار می دهد.

همیشه این اصل را رعایت کنید تا دچار مشکل نشوید: هیچگاه چیزی را که از انتشار آن در زندگی واقعی تان احساس امنیت و راحتی نمی کنید، در فضای مجازی منتشر نکنید، زیرا سرانجام کسانی که نباید، آن را خواهند دید.

حریم شخصی خود را مشخص کنید

در همه ی شبکه های اجتماعی این امکان را دارید که دسترسی افراد مختلف را به مشخصات فردی و محتوایی که منتشر می کنید، مشخص نمایید. در فیس بوک این امکان را دارید که بخش های مختلف اکانت تان را برای دوستان، دوستانِ دوستان، شبکه و همه افراد قابل دیدن کنید.

این موارد شامل برخی تنظیمات مهم بخش حریم خصوصی فیس بوک هستند:

- دوستان تان را گروه بندی کنید: فیس بوک این قابلیت را دارد که دوستان تان را براساس سطح روابط و صلاح دید خود در گروه های مجزا دسته بندی کنید. به طور معمول گروه‌ها در سه قالب دوستان، خانواده و کاری تقسیم بندی می شوند. در حالت دسته بندی، راحت تر می توان حریم خصوصی گروه ها را کنترل کرد.
  برای ایجاد لیست دوستان می توانید به صفحه ی Friends در فیس بوک مراجعه کنید. در این صفحه در برابر نام هر یک از دوستان تان گزینه ای با نام Add to List می‌بینید که با کلیک روی آن می توانید شخص مورد نظر را در یکی از لیست ها قرار دهید.

- اجازه دسترسی موتورهای جستجو را به پروفایل خود را متوقف کنید: برای عده ای از کاربران که می خواهند توسط نتایج جستجو در دسترس باشند و از آن استفاده ی تبلیغاتی کنند، این امکان بسیار ارزشمند است. اگر شما جزو این دسته از افراد نیستید، می توانید با مراجعه به صفحه ی Privacy و برداشتن تیک کنار گزینه Let other search engines link to your search engine indexing timeline مانع نمایش مشخصات تان در موتورهای جستجو شوید.

- از برچسب خوردن نام تان در عکس های نامناسب جلوگیری کنید: در فیس بوک می توان بر روی هر عکسی نام افراد مختلف را برچسب زد. زمانی که نام شما بر روی یک عکس چسبانده می شود، این عکس برای همه نمایش داده می شود. اینکه هر روز وقت زیادی را صرف حذف برچسب عکس ها کنیم، اصلا عاقلانه نیست. برای به آدرس زیر بروید (بجای username آی‌دی فیس‌بوک خودتان را بزنید)

https://www.facebook.com/**username**/allactivity?privacy_source=activity_log&log_filter=clus

و سپس روی چرخ‌دنده کوچیک بالا سمت راست کلیک کنید و گزینه Enable را انتخاب کنید.

از آلبوم هایتان محافظت کنید: شما می‌توانید با رفتن به صفحه آلبوم‌های ویدیویی و تصاویر خودتان، برای هر آلبوم یک سطح دسترسی مشخص کنید. تنها کافی است روی آیکون قفل در کنار هر آلبوم کلیک کنید و سطح دسترسی انتخابی خودتان را انتخاب کنید.

- اطلاعات تماس خود را خصوصی کنید: با مراجعه به Contact information از طریق کلید Info در قسمت پروفایل، می توانید برای هر بخش از اطلاعات خود دسترسی مشخصی را تعریف کنید. پس از انتخاب گزینه ی Edit روبروی عبارت Contact information، صفحه ای باز می شود که براساس گروه های از پیش تعریف شده دوستان، اجازه ی دسترسی به اطلاعات را برای هر کدام به تفکیک تعریف می کنید. البته برای این کار باید بر روی آیکن قفل روبروی هر کادر کلیک کنید و تنظیمات ویژه آن کادر را انجام دهید.

دسترسی افراد را به اکانت فیس‌بوک تان قطع کنید

هنگامی که فردی بدون اجازه و غیرقانونی به حساب کاربری تان وارد شود، می توانید ارتباط وی را قطع کنید. برای این منظور، بر روی گزینه ی Account در بالای صفحه ی پروفایل در سمت راست، کلیک کرده و از پنجره ای که باز می شود گزینه ی Account Settings را انتخاب کنید. اطلاعات مربوط به فعالیت های حسابتان را در گزینه ی Account Security خواهید یافت. اگر فرد دیگری هم log in شده باشد، همین اطلاعات در مورد او نوشته می شود و می توانید او را به عنوان ناشناس معرفی و ارتباطش را قطع کنید.

حتی ممکن است که کسی به حساب تان نفوذ نکرده باشد، بلکه روی کامپیوتر دانشکده، کتابخانه و یا کافی نت محله تان وارد حساب فیس بوک تان شده باشید، اما فراموش کرده باشید از آن خارج شوید. اینجا هم این کار حسابی به دردتان می خورد تا بعد از رفتن شما نفر بعدی نتواند از حساب تان استفاده کند.

سرقت اطلاعات شخصی، فیشینگ و اخاذی

ماهیت و طبیعت شبکه های اجتماعی، اجتماعی شدن و مراوده است. به این معنی که کاربران سپر زندگی روزمره را زمین می گذارند و بدون هیچ ملاحظه ای به گسترش ارتباطات شان می پردازند. با دوستان قدیمی شان تماس می گیرند و اطلاعات شخصی و عکس های خود را به اشتراک می گذارند.

خب نوبت بچه های بد است که علاقه ی فراوانی به مهندسی اجتماعی دارند. با حملات فیشینگ بسیار ساده، شما را شکار می کنند و به سوء استفاده می پردازند. به راحتی ماهیگیری درون یک آکواریوم!

حال نوبت استفاده از اکانت ها و اطلاعات شخصی سرقت شده است. احتمالا بسیاری از شما با پروژه ی کلاهبرداری سرمایه دار نیجریه ای آشنا هستید و دیگر با این شیوه کلک نخواهید خورد، ولی اگر یکی از دوستان قدیمی تان ایمیل بزند و یا در فیس بوک پیغام بدهد که در مسافرت است و کیفش را دزد برده و ماشین اش هم تصادف کرده، حالا برای برگشت نیاز به پول دارد، بعد از شما بخواهد که این پول را به حساب مسئول هتلی که در آن اقامت دارد بریزید، چه می کنید؟ به نظر کاملا واقعی می آید. دوستی از شما تقاضای پول کرده که برایتان بسیار عزیز است. به مشکل بدی هم برخورده است، پس شما وظیفه دارید که به او کمک کنید.

اما چند لحظه صبر کنید، اگر دوست تان اینقدر با شما صمیمی است که درخواست کمک و پول کند، چرا به شما تلفن نزده است؟ یعنی راهی سریع تر از فیس بوک و ایمیل برای درخواست کمک ندارد؟ گیرم شماره تان را گم کرده باشد، شما که می توانید به او زنگ بزنید و قبل از هرگونه واریزی، تلفنی تایید این درخواست را بگیرید!

چگونه ممکن است که درخواست یک دوست تقلبی از کار درآید؟ خب، یک هکر زرنگ اکانت فیس بوک یا توییتر دوست تان را سرقت کرده و از آن طریق، ایمیل او را هم به دست آورده است. دوست شما هم که با اعتماد به نفس کامل، رمز عبور یکسانی را برای همه حساب های اینترنتی اش انتخاب کرده است. پس شما درخواست کمکی را دریافت می کنید که شماره حساب اعلام شده در آن هم متعلق به هکر مهربان داستان ما است.

آنچه در پشت آدرس های کوتاه پنهان است

در بقیه درس های این مجموعه آموزشی به طور مفصل به آدرس های کوتاه شده و سایت های کوتاه کننده آدرس خواهیم پرداخت، فقط حواس تان باشد که به دلیل محدودیت ۱۴۰ کاراکتری توییتر، با اینگونه آدرس ها زیاد برخورد خواهید داشت. استفاده از آنها در پست های فیس بوک و فرندفید هم زیاد شده است. پس مراقب آدرس های خطرناکی که ممکن است در آنها پنهان شده باشند و شما را ناخواسته به آدرس های خطرناکی منتقل کنند، باشید.

پاک کردن حساب کاربری در سایت ها و شبکه های اجتماعی

همه ی ما عضو تعداد زیادی از سایت ها و سرویس های آنلاین و شبکه های اجتماعی هستیم و گاهی همه ی اینها کمی طاقت فرسا و دردسرساز می شوند. گاهی اوقات، چه برای ساده کردن زندگی مان، یا چون از سایت یا سرویس خاصی خسته شده ایم، لازم است که عضویت مان در برخی سایت ها را حذف کنیم.

چیزی که اغلب موقع ثبت نام در این گونه سایت ها توجهی به آن نداریم، این است که چقدر پاک کردن دائمی حساب کاربری مان مشکل است. برخی از آنها نیازمند یک پروسه پیچیده و چندگانه هستند که ممکن است چند روز (یا هفته) طول بکشد.

فیس بوک

اگر فقط می خواهید حساب تان را برای مدتی مسدود کنید و امکان این را داشته باشید که بعدا دوباره از آن استفاده کنید، می توانید حسابتان را غیرفعال کنید. این کار ساده است: فقط به قسمت Account Settings بروید و بر روی لینک «deactivate account» کلیک کنید. با این کار فورا حسابتان برای دیگر افراد در فیس بوک نامرئی می شود. اگر هم روزی تصمیم گرفتید که دوباره حسابتان را فعال کنید، به همین سادگی کار انجام می شود و تنها کافیست که بر روی «activate account» کلیک کنید.

اگر دنبال چیزی می گردید که کمی دائمی تر باشد، لازم است درخواستی برای فیس بوک ارسال کنید. اگرچه نکته نیرنگ آمیز این است که آنها بلافاصله حساب شما را پاک نمی کنند. اگر در طول زمانی که قرار است حذف دائم حساب تان صورت بگیرد شما وارد فیس بوک شوید، یا هر ارتباطی با

فیس بوک برقرار کنید، درخواست حذف تان لغو می شود. برای درخواست حذف شدن حساب تان می توانید از این فرم استفاده کنید. به خاطر داشته باشید که بعد از آن دیگر وارد حساب کاربری تان نشوید. گزارش های غیر رسمی می گویند این کار ۱۴ روز وقت می برد. برای اینکه مطمئن شوید، ممکن است یک ماه یا بیشتر لازم باشد صبر کنید و بعد تلاش کنید که وارد حساب کاربری تان شوید، تا مطمئن شوید که پاک شده است.

توییتر

پاک کردن حساب کاربری در توییتر در مقایسه با فیس بوک نسبتا آسان تر است. تمام کاری که باید بکنید، این است که وارد Account Settings بشوید و بر روی گزینه ی «Deactivate my account» در آخر صفحه کلیک کنید. این غیر فعال سازی دائمی است. اگرچه ممکن است یک ماه طول بکشد تا حساب و اطلاعات شما بطور کامل از سیستم توییتر حذف شود. اگر می‌خواهید در مورد توییتر اطلاعات بیشتری کسب کنید، می‌توانید در دوره توییتر درسنامه ثبت نام کنید.

درس چهاردهم – امنیت فیزیکی و امنیت در محیط کار

هرگاه در یک مبحث مربوط به کامپیوتر صحبت از امنیت به میان می آید، بسیاری به فکر جلوگیری از نفوذ ویروس ها و تروجان ها، مقابله با حملات فیشینگ و محافظت های نرم افزاری می افتند. اما هر مقدار که برای داشتن آنتی ویروس قوی و به روز، فایروال قدرتمند، رمزهای عبور قرص و محکم و برنامه های نرم افزاری هزینه کنید، باز هم یک سارق می تواند در اتاق کامپیوتر و یا شرکت تان را باز کرده و از اطلاعات شما کپی برداری کرده و یا سیستم های شما را بدزدد! بنابراین آخرین درس این دوره به امنیت فیزیکی اختصاص یافته است تا هیچ وقت این بخش کار را فراموش نکنید.

شاید به جرات بتوان گفت که پایه ی هر برنامه و طرح حفاظتی، امنیت فیزیکی است. اگر در شرکت قفل و بند درستی نداشته باشد و یا کلید آن در اختیار همه باشد، خرید برنامه های امنیتی چند صد هزار تومانی هم دردی را دوا نخواهد کرد.

در این درس به برخی نکات ضروری در خصوص امنیت فیزیکی می پردازیم:

از قفل های مطمئن داخلی برای درهای ورودی اصلی استفاده کنید

اول از همه باید به فکر زمانی باشیم که در خانه یا شرکت نیستیم. مطمئن هستید که درهای ورودی به اندازه ی کافی ایمن هستند و به خوبی بسته می شوند؟ بهتر است که در ورودی شرکت یا خانه فلزی باشد. علاوه بر قفل های آویز معمولی، آن را به قفل داخلی هم مجهز کنید. این قفل ها که به قفل های گاوصندوقی هم مشهور هستند، درون در نصب می شوند و معمولا دو یا چهار زبانه بلند دارند که داخل لنگه مقابل در چفت می شود.

حتی اگر بخش آی تی و محل قرارگیری کامپیوترهای شما در قسمت مجزایی از محل کارتان است، در ورودی آن را هم به چنین قفلی مجهز کنید تا امکان نفوذ هنگام عدم حضور شما بسیار کاهش یابد.

در اتاق کامپیوتر همیشه قفل باشد

هنگام انتخاب اتاقی برای نگهداری کامپیوتر و تجهیزات شبکه، قبل از توجه به زیبایی و شیک بودن اتاق، ابتدا به در آن توجه کنید. آیا محکم و قابل اطمینان است؟ آیا دارای قفل و بند درست و حسابی است و به خوبی قفل می شود؟ حال به عنوان یک قانون برای همه ی افرادی که از این اتاق استفاده

می کنند، همیشه در باید قفل باشد. عادت کنید که حتی هنگام ترک اتاق برای چند دقیقه، در را قفل کنید. شاید سختگیرانه و مشکل به نظر برسد، اما برای یک دزد اطلاعات حرفه ای تنها چند دقیقه زمان برای سرقت یک هارد یا کپی برداری از اطلاعات بر روی کول دیسک کافی است. برای اضافه کردن ابزاری به روتر، برای استفاده بعدی و یا نصب کی‌لاگرهای سخت افزاری هم که حتی یک دقیقه زمان زیادی به نظر می رسد.

اتاق کامپیوتر قلب فیزیکی شبکه ی کامپیوتری شرکت شما است. یک بدخواه با دست یابی به این اتاق، به راحتی با دستکاری سوییچ ها، روترها، کابل ها و دیگر ابزارها می تواند صدمات سختی را وارد آورد.

یک سیستم نظارت و مراقبت دائمی داشته باشید

درست است که قفل کردن در، راه کار بسیار مناسبی است اما اگر فردی که اجازه ی ورود و امکان دسترسی داشته باشد و بخواهد دست به خرابکاری بزند، یا فردی با شکستن در و تخریب قفل آن وارد شود، چگونه وی را شناسایی می کنید. بهترین راه داشتن یک سیستم کنترل تردد به اتاق است. این سیستم می تواند یک قفل با کارت مغناطیسی یا رمز و شاید یک دستگاه شناسایی هویت بیومتریک باشد. در هر صورت تمامی ورود و خروج ها با درج زمان دقیق ثبت و نگه داری می شوند. اگر امکان چنین هزینه هایی ندارید، یک دوربین ویدیویی نیز می تواند نیاز شما را برطرف کند. یک دوربین کوچک ویدیویی را در محلی که به راحتی قابل دیدن و از کار انداختن نباشد، به گونه ای نصب کنید که تصویر کاملی از ورودی اتاق یا ساختمان ضبط کند. حال شما در موقع لزوم می توانید ورود و خروج های صورت گرفته را کنترل کنید. حتی با کمی هزینه ی بیشتر می توانید از دوربین هایی استفاده کنید که علاوه بر ضبط تصاویر، از طریق ایمیل یا پیام کوتاه شما را خبر کنند.

تمامی ابزارهای در معرض خطر، در محل امنی قرار داشته باشند

ممکن است کامپیوتر مرکزی شرکت خود را در اتاق امنی گذاشته و با رمز عبور قوی و نرم افزارهای لازم از آن مراقبت کنید. اما روتر، هاب، یا سوییچ های شبکه تان در کجا قرار دارند؟ یک هکر به راحتی با یک لپ تاپ و دسترسی به هاب قادر است خسارات شدیدی را به شما وارد کند. تا حد ممکن تمامی ابزارهای شبکه تان را در اتاق های مطمئن و قفل شده قرار دهید. اگر هم امکان چنین

کاری را ندارید، حداقل آنها را درون جعبه های محکم و قفل داری قرار دهید که هر کسی نتواند به آنها دسترسی داشته باشد.

محیط کاری را فراموش نکنید

هکر می تواند از هر ابزار و دستگاه ناامن موجود در محیط کارتان برای نفوذ به شبکه و تخریب و سرقت اطلاعات استفاده کند. اتاق و میز کارمندی که به مرخصی رفته یا اخراج شده و کسی به آنجا سر نمی زند، بهترین طعمه برای یک هکر خبره است. دسترسی کامپیوتر و ابزارهای بلا استفاده به شبکه را قطع کنید و یا آنها را به انباری منتقل کنید. در اتاق های خالی را قفل کنید. از کارکنان بخواهید حتی وقتی برای نهار بیرون می روند، درها را قفل کنند. اگر در خانه جشن یا برنامه ای دارید که همه ی شرکت کنندگان آن را نمی شناسید، حتما در اتاق کامپیوتر قفل شده باشد. استفاده از قفل های سخت افزاری از قبیل قفل پورت USB و شبکه هم فکر خوبی است.

کیس کامپیوترتان را قفل کنید

وضعیتی را در نظر بگیرید که جناب دزد به هر شکلی که شده به کامپیوتر شما دست پیدا می کند. حال باید به راحتی پیچ های پشت کیس را باز کند و هارد دیسک را بردارد و برود؟ یا اینکه هر بار از اتاق بیرون می روید هارد دیسک را درون جیب تان می گذارید و با خودتان می برید؟ امروزه در پشت همه کیس ها جایی برای استفاده از قفل تعبیه شده است. پس با کمی هزینه حتما کیس های تان را قفل کنید، تا برای سرقت هارد دیسک به چیزی بیش از یک پیچ گوشتی نیاز باشد.

مراقب ابزارهای پرتابل باشید

لپ تاپ ها و تبلت ها می تواند خطری بالقوه برای اطلاعات شما باشند. تا حد امکان هیچگونه اطلاعات مهم و حیاتی را بر روی ابزارهای اینچنینی نگهداری نکنید، زیرا حداقل رمز عبور شبکه بی سیم تان بر روی همه ی این ابزارها ذخیره شده است. پس برای لپ تاپ ها حتما کابل های قفل تهیه کنید یا اینکه آنها را در کشو یا کمدی امن نگه دارید یا حتی به عنوان یک روال کاری همه موظف باشند که همیشه ابزارهای شان را به همراه داشته باشند.

نگهداری امن نسخه های پشتیبان

یکی از مهمترین کارهای هر فرد یا شرکتی تهیه ی نسخه های پشتیبان از اطلاعات است. اما محل نگهداری نسخه های پشتیبان هم از اهمیت بالایی برخوردار است. اگر آنها را در همان اتاق کامپیوتر بگذارید که ممکن است به راحتی دزدیده شوند و یا در اتفاقاتی مانند آتش سوزی از بین بروند، کل برنامه ی پشتیبان گیری شما بی مصرف خواهد بود. بهتر است که نسخه ای از بک آپ ها را به صورت رمزگذاری شده و در جای مطمئنی خارج از محل کارتان نگهداری کنید.

اگر کارمندان تان هم به بک آپ گیری اطلاعات روی سی دی، کول دیسک یا هارد های اکسترنال عادت دارند، حتما آنها را به گونه ای آموزش دهید که اطلاعات را همیشه به صورت رمزگذاری شده و امن نگه داری کنند.

مراقب دستگاه های کپی و پرینتر باشید

در نگاه اول یک دستگاه کپی یا پرینتر نمی تواند خطری برای امنیت اطلاعات محسوب شود، اما متاسفانه دستگاه های کپی و پرینت امروزی، نسخه ای از اطلاعات چاپ شده را درون هارد و یا حافظه داخلی خود نگه می دارند. کافی است که فردی این دستگاه را بدزدد و با کمی تلاش به اطلاعات موجود در آن دست یابد تا نسخه ای از مطالب چاپی شما را در دست داشته باشد. بهتر است که این دستگاه ها را تا حد ممکن در اتاق های امن نگه داری کنید و یا آنها را به شکلی نصب کنید که به راحتی قابل حمل و سرقت نباشند.

علاوه بر این برگه های چاپ شده توسط این دستگاه ها هم خطر بالقوه دیگری هستند، همیشه نسخه های چاپی هستند که به درد نمی خورند و راهی سطل زباله می شوند. این کپی ها به راحتی قابل سرقت و سوء استفاده هستند. به عنوان یک سیاست کاری حتی کاغذهای معمولی و بی اهمیت را هم به جای سطل زباله، راهی دستگاه کاغذ خرد کن کنید. این باعث می شود که همه به این کار عادت کنند و هیچ کپی مهم بی مصرفی به دست افراد سوءاستفاده گر نیافتد.

از سیستم های هشداردهنده استفاده کنید

قفل های مطمئن و در و پنجره های محکم جلوی ورود سارقان را می گیرند. اما استفاده از یک سیستم هشدار دهنده برای امنیت بیشتر امری ضروری است. اولین کاربرد یک سیستم هشدار

دهنده ترساندن و فراری دادن دزدها است. علاوه بر این شما را با خبر می کند که اتفاقی افتاده است.

یک سیستم دزدگیر معمولا از تعدادی سنسور حساس به حرکت، سنسور شکست شیشه و یک سیستم کنترل مرکزی تشکیل شده است. پس از اینکه حرکت غیر مجازی تشخیص داده شود، علاوه بر به صدا در آمدن آژیر، دستگاه با شما و پلیس تماس تلفنی برقرار خواهد کرد.

مراقب کلیدهایتان باشید

امروزه ابزارهای امنیتی و حفاظتی بسیار پیشرفته ای در اختیار کاربران قرار دارد، ولی با این وجود هنوز همین کلیدهای فلزی کوچک، حفره ی امنیتی بزرگی محسوب می شوند. خانه یا محل کار شما تعداد زیادی در و قفل دارد و همه ی آنها برای باز شدن به کلید نیاز دارند. آیا همه ی افرادی را که این کلیدها را در اختیار دارند می شناسید؟ آیا می دانید که آنها چند کپی از کلیدهای شان دارند؟

کپی کردن یک کلید، کار چندان سختی نیست و تنها کافی است دارنده ی کلید به یک قفل ساز مراجعه کند. حتی یک سارق متبحر می تواند با یک تکه موم یا خمیر بازی طرح کلید را دزدیده و نمونه ای از آن بسازد. استفاده از کلیدهای چهار پهلو و کلیدهای موسوم به کامپیوتری (که به جای دندانه سوراخ هایی بر روی خود دارند) هم ایده ی خوبی به نظر می رسد. به هر حال کلیدسازان کمی قادر به کپی کردن آنها هستند و دزدیدن طرح آنها با خمیر بازی اگر نگوییم غیر ممکن، حداقل خیلی سخت است.

پس همیشه مراقب باشید که کلیدها دست چه کسانی هستند و هیچ گاه موضوع یک کلید گم شده را ساده نگیرید. با کم شدن هر کلید هم بهتر است به فکر استفاده از قفل جدید برای آن محل بود. بعد از خواندن این همه درس و آزمون فراموش نکنید که امنیت سخت افزاری را هم جدی بگیرید.

موفق باشید.

مرجع گردآوری مطالب: سایت درسنامه

گردآوری و تنظیم: نکات کوچک

نکات کوچک www.tinytips.ir