اشتباه امنیتی متعارف که می توانند حریم خصوصی و پول شما را به خطر اندازند

تا چه حد آسیب‌پذیرید؟ از هرکس که می‌خواهید بپرسید که آیا زمانی که مورد حمله قرار گرفت، غافلگیر شده‌است؟ مطمئن باشید که جوابش مثبت است. در بیشتر موارد دزدها شب هنگام که خوابید حمله می‌کنند؛ دلیل کاملا واضح است !درست زمانی که کمترین هوشیاری و آمادگی را دارید. اما حتی هنگامی که بیدارید هم ممکن است کاری کنید که امنیت شما را به خطر اندازد، به طوری که در واقع از هکرها دعوت می‌کنید تا به شما آسیب برسانند.

حریم خصوصی و پول مسلما مهمترین چیزی هستند که معنای امنیت را کامل می‌کنند. همه ما می‌خواهیم از هویت مان، حریم خصوصی مان، و در نهایت از پول‌های مان محافظت کنیم. هیچ کس دوست ندارد روزی که حساب بانکی خود را چک می‌کند در عین ناباوری عدد صفر را ببیند!

در مقاله پیشِ‌رو مهمترین اشتباهات امنیتی که ممکن است توسط تمامی کاربران رایانه در سراسر جهان انجام شوند را بررسی خواهیم کرد. غفلت از هرکدام، حفره‌ای آسیب‌پذیر به روی افراد سودجو باز خواهد کرد و گامی‌ست به سوی از دست رفتن هویت، حریم خصوصی و سرمایه‌تان.

اشتباه اول: عدم به روز رسانی ضد بد افزار(Anti-Malware)

این یکی از شایع‌ترین نکات امنیتی است که معمولا دیده می شود: یک برنامه ضد بدافزار نصب کنید و آن را به روز نگه‌دارید! دقیقا در عین مهم بودن این نکته، خیلی‌ها آن را نادیده می‌گیرند. اگر در حال خواندن این مقاله هستید و هیچ برنامه ضد ویروس یا ضد بدافزاری روی رایانه‌تان نصب نیست، بی‌درنگ خواندن را کنار بگذارید و همین حالا آن‌ها را نصب کنید! در اینترنت می توانید انواع مختلف ضد بدافزارهای عالی و البته رایگان را بیابید.

البته که داشتن یکی کفایت می‌کند! به شرط اینکه مرتبا آن را به روز نگه‌دارید. اکثر این نرم‌افزارها طبق برنامه زمان‌بندی مشخصی به روز رسانی می‌شوند. پس هیچ‌وقت جلوی آپدیت شدن آن‌ها را نگیرید. زیرا اگر چنین کاری کنید همان بهتر که اصلا ضد بدافزاری نداشته باشید!

اشتباه دوم: عدم استفاده از فایروال

تعداد کسانی که از ضد بدافزار استفاده می‌کنند کم است. تعداد کسانی که هم از ضد بدافزار و هم از فایروال استفاده می‌کنند کمتر! ممکن است بپرسید "آیا باید از هر دو آن‌ها استفاده کنم؟" و جواب کاملا روشن است: "بله ."!فایروال و ضد بدافزار به هیچ‌عنوان یکی نیستند! آن‌ها دو هدف کاملا متفاوت دارند و از همین جهت شما باید از هر دو برای امنیت بیشتر استفاده کنید.

این طور فکر کنید که فایروال نرده‌های مزرعه شما هستند و ضد بدافزار، اسلحه ای در دستان تان! نرده جلوی بسیاری از مزاحمان را می گیرد. ولی ممکن است رخنه‌هایی داشته باشد که بعضی میهمانان ناخواسته بتوانند از آن عبور کنند و مجبور باشید خودتان شخصا وارد عمل شوید.

دقیقا مانند مثال بالا، یک فایروال می‌تواند خیلی از ناخواسته‌ها را دور کند، ولی وقتی که یک تروجان یا ویروس خاصی پیدا شود، میدان را خالی می‌کند و اینجاست که ضد بدافزار بدردتان می‌خورد.

اشتباه سوم: عادت‌های ایمیلی غیر ایمن

بعد از چندین و چند سال، و پس از ورود وبلاگ‌ها و شبکه‌های اجتماعی و دیگر چیزها، هنوز هم ایمیل پرمصرف‌ترین راه ارتباطی در دنیای مجازی است و از همین‌رو پرمصرف‌ترین راه برای کلاه‌برداران! این روزها از دست دادن خیلی چیزها با یک ایمیل تقلبی بسیار شایع است.

از کلاه‌برداری‌های فیشینگ دوری کنید! یاد بگیرید که چگونه آن‌ها را بشناسید و در دام شان نیفتید. وقتی ایمیلی ناخواسته و ناشناس گرفتید که به نظر عاری از جزئیات آشناست، اصلا بازش نکنید. اصلا جوابش ندهید. مستقیما آن را پاک کنید. سوالی که پیش می‌آید این است که اساسا چگونه این ایمیل‌ها را بشناسیم؟! اولین راه این است که دنبال شماره تلفن‌ها و نشانی‌های تقلبی بگردید. تکرار برخی کلمات و قواعد دستوری راه دیگر لو رفتن این دست ایمیل‌ها است. و راه دیگر هم شک کردن به فرستنده ناشناس است.

اشتباه چهارم: رمزهای عبور غیر هوشمندانه

بله! رمزعبور از همه چیز مهم‌تر است. دقیقا همان چیزی که هنوز هم خیلی‌ها توجه باید و شاید به آن نمی‌کنند و هنوز هم تعداد کسانی که از 123456 استفاده می‌کنند باور نکردنی‌ست !

استفاده از یک رمزعبور واحد برای تمام زندگی مجازی‌مان کار درستی نیست . فکر کنید که کلید خانه‌تان با کلید محل‌کارتان، گاوصندوق‌تان و حتی ماشین‌تان یکی باشد. مضحک است!

و اما راه حل عاقلانه. استفاده از کلیدهای متفاوت برای درهای متفاوت .اما فقط این نیست. اگر امنیت بیشتر می‌خواهید، هر 6 ماه یک‌بار کل قفل ها را عوض کنید.

اشتباه پنجم: پخش کردن اطلاعات شخصی

تاکنون در فیلم‌های کمدی و خنده‌دار دیده‌اید که شخصی از روی ناآگاهی اطلاعاتی بسیار مهم را فاش کند؟ ممکن است بر روی پرده سینما بسیار خنده‌دار باشد؛ ولی وقتی در زندگی واقعی اتفاق بیفتد...

در دنیای بازی‌های رایانه‌ای، معمولا هکرها دقیقا نزدیک‌ترین افراد به شخص صاحب حساب هستند. رمزتان را به آن‌ها می‌دهید تا آن‌ها هم بتوانند بازی کنند. در اول همه چیز طبق روال عادی است. ولی بعد از مدتی هر چه دارید به باد می‌رود. تا وقتی که در دنیای بازی و سرگرمی باشد، ممکن است چندان هم مهم نباشد، ولی وقتی همین اتفاق برای جیمیل، و سایر حساب‌های کاربری‌تان بیفتد دیگر نمی‌توان با بیخیالی از آن گذشت.

یا شاید بسیار تصادفی شماره کارت بانکی‌تان را به کسی نشان بدهید و اصلا هم برای تان مهم نباشد؛ چون او دوست شماست. ولی هیچ‌وقت آن‌قدرها هم مطمئن نباشید.

بهترین راه این است که هر چیزی را که به نظرتان شخصی و خصوصی است، خصوصی و محرمانه نگه‌دارید. مثل رمزهای عبور، تلفن، آدرس، شماره‌ی کارت بانکی و...

هرکدام از موارد یاد شده در این مقاله می‌توانند تمام زندگی شما را نابود کنند. ممکن است پیش از این اطلاعات مهمی را به دیگران نشان داده باشید و یا از رمزعبوری که 10 سال پیش انتخاب کرده بودید، هنوز هم استفاده می‌کردید و هیچ اتفاقی هم برای تان نیفتاده باشد. چه خوب! مایه شادمانی‌ست که تا این حد خوش شانس هستید. ممکن است ساعت‌ها درب خانه‌تان را سهوا باز گذاشته باشید و هیچ اتفاق بدی هم نیفتاده باشد. اما آیا این کار عاقلانه است؟

از این اشتباهات بپرهیزید و مطمئن باشید که اگر مراقب باشید، هیچ اتفاقی برای تان نمی‌افتد. ایمن بمانید!

منبع : http://www.esecurity.ir/