الزامات امنیتی فناوری اطلاعات

- ## انتخاب نام کاربری و گذر واژه مناسب:

امروزه برای حفظ اطلاعات و امنیت بیشتر در دنیای کامپیوتر و اینترنت، استفاده از نام کاربری (*User*) و کلمه عبور (*Password*) مناسب، انکار ناپذیر می باشد. در این شرایط اغلب نفوذگران، صرفاً با وقت گذاشتن بر روی کشف کلمه عبور، به سیستم ها نفوذ می کنند. لذا بهتر است برای انتخاب کلمات عبور، موارد ذیل مدنظر قرار گیرد:

۱. یک کلمه عبور، می باید شامل حداقل هشت کاراکتر باشد. مطمئن باشید که حدس زدن کلمات عبور که کوتاه تر هستند، برای هکرها بسیار ساده است، ضمن اینکه در زمان کمتری به کشف آن نائل می شوند.

۲. کلمات عبور شامل حروف انگلیسی بزرگ و کوچک a تا z و A تا Z و اعداد ۰ تا ۹ و حداقل یک علامت غیر الفبایی مثل % @ $ باشند.

۳. هیچ گاه در کلمات عبور، از حرف یا کلمات پشت سر هم یا متوالی (چه از نظر الفبایی و چه بر اساس موقعیت روی صفحه کلید) استفاده نکنید. به عنوان مثال کلمات، " asdfghkl "، "۳۴۵۶۷۸۹ " ، " abcdefg"مناسب نیستند.

۴. تمامی کاراکتر های کلمه عبور، نباید فقط حرف یا فقط کلمه باشند.

۵. از استفاده مجدد یا تکرار کلمات عبور قدیمی، جداً بپرهیزید.

۶. برای سامانه های مختلف از کلمات عبور یکسان استفاده نکنید.

۷. کلمات عبور را در دوره های کوتاه مدت تغییر دهید.

- ## اهمیت حفظ اطلاعات شخصی از جمله شناسه کاربری و گذرواژه:

این روزها که همه اطلاعات در دنیای مجازی در هم تنیده شده و باید برای انجام کارهای ضروری و غیرضروری خود اعم از کارهای بانکی، ارسال پیام و غیره از اینترنت، اپلیکیشن و حساب‌های کاربری متعدد خود در فضای مجازی استفاده کنیم، آگاهی از اینکه چگونه از اطلاعات شخصی و حریم خصوصی خود محافظت کنیم و امنیت سایبری حساب‌های کاربری خود را افزایش دهیم، کمک به سزایی خواهد کرد.

در این شرایط :

۱.برای بالا بردن امنیت خود از دادن اطلاعات شخصی ار جمله شناسه کاربری و گذرواژه(رمز عبور) خود به سایر افراد جداً اجتناب کنید.

۲.از نوشتن رمز عبور بر روی کاغذ و گذاشتن آن بر روی میز محل کار، نزدیک کامپیوتر و یا چسباندن آن بر روی کامپیوتر، جداً خودداری کنید.

۳.تعداد زیادی از برنامه‌ها امکان به خاطر سپردن رمزهای عبور را ارائه می‌کنند، زمانی که سیستم را ترک می‌کنید این قابلیت را غیر فعال کنید.

۳. از کلمات قابل حدس زدن همچون نام، نام خانوادگی، سال و تاریخ تولد، نام همسر و غیره برای نام کاربری یا کلمه عبور، اکیداً خودداری کنید و در صورتی که می‌خواهید از این کلمات، عبارات و اعداد استفاده کنند، باید در میان آن از حروف اختصاری و نشانه‌گذاری استفاده کنید.

۴. هر نوع شناسه کاربری و گذر واژه (رمز) اعم از ثابت، یکبار مصرف، پیامکی و ... که مخصوص شماست را به هیچ عنوان و هیچ دلیلی به دیگران بازگو ننمایید. این رمزها فقط مخصوص شما و برنامه های شماست و بازگو نمودن آن برای دیگران، می تواند از هر نظر شما را دچار ضرر و زیان نماید.

۵. سعی کنید اطلاعات شخصی خود را بر روی شبکه های اجتماعی به اشتراک نگذارید. مجرمین سایبری با روشهای مهندسی اجتماعی، می توانند اطلاعات رمز های شما را از این طریق حدس بزنند و شما را دچار زیان نمایند.
۶. در صورت داشتن تماس یا پیامهایی مبنی بر برنده شدن یا مصاحبه تلفنی در شبکه های تلویزیونی و ... به هر طریق، هیچگونه اطلاعات شخصی یا بانکی خود و همچنین کدهایی که از طریق پیامک دریافت می کنید را در اختیار مخاطب قرار ندهید.

- ## استفاده از آنتی ویروس ها در هنگام بهره برداری از خدمات بانکداری الکترونیکی:

شاید روزگاری بدافزارها را فقط افراد تازه کار می‌نوشتند اما حالا مجرمین سایبری به دنبال خالی کردن حساب‌های افراد و کسب درآمد از راه‌های غیر قانونی هستند. در این خصوص شاهد گونه‌ای از بدافزارها با عنوان «بدافزارهای مالی (*Financial Malware*) » هستیم که از آنها به عنوان بدافزاری بانکی نیز یاد می‌شود. اگر بخواهیم ساده بگوییم، بدافزارهای مالی گونه‌ای خاص از بدافزارها هستند که سیستم و حتی شبکه‌های اینترنتی را با هدف دستیابی به اطلاعات حساب‌های مالی، سرقت اطلاعات کارت‌های بانکی و حتی کلاه‌برداری پویش می‌کنند. این بدافزارها بسیار هوشمندانه طراحی می‌شوند تا نه تنها قربانی متوجه حضور آنها نشود، بلکه از چشم آنتی ویروس‌ها نیز پنهان بمانند.

لذا نکات ذیل را مد نظر قرار دهید :

۱.سعی کنید در تمامی دستگاههای رایانه ای خود اعم از کامپیوتر شخصی، لپ تاپ، تبلت، گوشی و ... از آنتی ویروس معتبر استفاده کنید.

۲. آنتی ویروس خود را هر چند وقت یکبار به روز رسانی کنید.

۳. سعی کنید از آنتی ویروسهای رایگان که بر روی سایت های غیر معتبر وجود دارد، استفاده نفرمایید.

۴.قبل از اتصال حافظه های جانبی به سیستم خود، محتویات آنها را با آنتی ویروس کنترل کنید تا از غیر ویروسی بودن آنها مطمئن شوید.

۵.به هیچ عنوان فایلهای آلوده را بر روی سیستم های خود باز نکنید. این فایلهای آلوده می توانند از فلش، ایمیل یا شبکه های اجتماعی نیز به شما ارسال شود. در نتیجه مراقب باشید.

۶. برخی تصاویر یا فایلهای صوتی پر حجم می تواند شامل فایلهای آلوده باشند. در نتیجه حتما آنها را با آنتی ویروس کنترل کنید.

- ## اطلاع رسانی در خصوص تارنماها و پست های الکترونیکی جعلی، فیشینگ و نظایر آن:

کاربران باید به منظور حفاظت از اطلاعات شخصی و مالی خود از درگاه‌ها و نرم افزارهای ایمنی که بانک‌ها برای کاربرانشان تعبیه کرده‌اند، استفاده کنند. در این میان روشی موسوم به فیشینگ وجود دارد که برای جمع آوری اطلاعات شخصی و مالی افراد از طریق ایمیل ها و وب سایت های فریبنده اقدام می نماید.

در نتیجه توجه به نکات ذیل ضروری می باشد:

۱.سایتهایی که در ابتدای آدرس وب سایت از عبارت *https* با پسوند s (حرف نخست کلمه *secure*) استفاده می‌کند اغلب دارای امنیت بوده و معمولا وب سایتهایی که امن و معتبر نیستند، از عبارت *http* بدون حرف s استفاده می‌کنند. بدون شک، توجه به این کلمات و عبارات در ابتدای آدرس وب سایت مربوطه می‌تواند تا حد زیادی شما را از ورود به سایت‌های نامعتبر و جعلی دور کند.

۲.به آدرس وب سایت توجه کنید . در این خصوص مثلا آدرس اصلی وب سایت بانک صادرات *https://www.bsi.ir* یا مثلاً آدرس بانکداری الکترونیک *https://ib.bsi.ir* یا نسخه همراه بانک وبی به نشانی *https://eb.bsi.ir* می باشد. لذا هر آدرس مشابه دیگری، بانک صادرات نبوده و باید به آن دقت نمود.

۳.برای دستیابی به خدمات الکترونیک یا درگاههای پرداخت، دقت کنید آدرس شاپرک به نشانی **نام درگاه پرداخت نقطه(.)** و در ادامه دقیقاً آدرس *shaparak.ir* ختم گردد.

۴. عدم نمایش تصویر قفل، یا نمایش قفل به رنگ قرمز یا با خط قرمز، یا پیغام خطا با مضمون امنیتی و خطای SSL هنگام بارگذاری صفحه درگاه پرداخت، از نشانه های درگاه های غیرمجاز و ناامن است.

۵. اگر آدرس سایت پرداخت نامعتبر باشد یا از طریق کلیک روی یک لینک به آن وصل شده اید، به هیچ وجه اطلاعات مالی و بانکی خود را در آن وارد ننمایید. ممکن است وب سایت یا درگاه جعلی باشد.

۶. بهتر است از درگاههای پرداخت که از طریق ایمیل ما را به صفحه پرداخت هدایت می کند، استفاده ننماییم.

۷.حتماً نرم افزارهای بانکی مربوط به بانک صادرات ایران را از سایت بانک به نشانی *https://www.bsi.ir* دریافت و نصب نمایید. چرا که احتمال انتشار نسخه های جعلی برنامه های بانک، در بقیه سایت ها یا فروشگاههای اینترنتی نرم افزار وجود دارد.

- ## عدم استفاده از کامپیوترها و شبکه های عمومی پرخطر برای استفاده از خدمات الکترونیکی:

یکی از خدمات شهری رایگان که در شهرهای بزرگ جهان وجود دارد، ارائه سرویس اینترنت همگانی، رایگان و باز است که به عقیده بسیاری از منتقدان، از مهم‌ترین راه‌های نفوذ هکرها و دسترسی مجرمان سایبری به اطلاعات شخصی ذخیره شده در رایانه و گوشی هوشمند کاربران به شمار می‌آید. لذا :

۱.بهترین راهکاری که همواره پیشنهاد می‌شود، آن است که تنها به شبکه‌های اینترنت بی‌سیم وای فای معتبر در خانه و سرکار خود متصل شوید و یا در صورت لزوم، از اینترنت دیتای تلفن همراه استفاده کنید.

۲. در هنگام بهره گیری از خدمات الکترونیکی بانکی به هیچ وجه از شبکه های عمومی اینترنت بهره گیری ننمایید.

۳. حتی اگر از دستگاههای شخصی خود استفاده می کنید و به شبکه خانگی متصل هستید، در صورت استفاده از نرم افزار های *VPN* به شبکه عمومی نا امن متصل می شوید. پس بهتر است که قبل از استفاده از خدمات و برنامه های بانکی، از خاموش بودن *VPN* اطمینان حاصل نمایید.

- ## خروج صحیح از صفحات تارنما سامانه بانکداری الکترونیک بانک صادرات ایران:

جهت امنیت بیشتر در هنگام بهره گیری از خدمات الکترونیکی و خصوصاً در صورتی که از رایانه ای بهره می گیرید که مالک آن نمی باشید، در زمان ورود در صورتی که مرورگر از شما درخواست ذخیره نام کاربری و رمز عبور را می نماید، قبول ننموده و پس از اتمام فعالیت خود در تارنمای سامانه بانکداری اینترنتی، با انتخاب گزینه خروج در قسمت فوقانی سمت چپ صفحه از کاربری خود خارج شوید.