مدیریت فناوری اطلاعات
اداره امنیت توسعه و یکپارچه سازی سیستم ها
دایره امنیت سیستم ها

آگاهی رسانی امنیتی به کاربران خدمات الکترونیکی

شهریور ماه ۱۳۹۰

v نکات مربوط به امنیت پسورد اینترنت بانک و دیگر خدمات الکترونیکی

۱- پسورد باید به گونه‌ای انتخاب شود که دیگری نتواند آن را از روي مشخصات شخصي کاربر مانند سال تولد، نام فرزند، شماره شناسنامه، شماره موبایل، تلفن منزل و غیره حدس بزنند.

۲- برای انتخاب پسورد تا حد امکان از کلمات معنادار استفاده نکنید. بهتر است ترکیبی از انواع متفاوت کاراکتر ها به کار رود. برای مثال (PqoW!@#)

۳- هر کاراکتری که شما به رمز عبور خود اضافه می کنید، حفاظت ایجاد شده به وسیله آن را چندین برابر افزایش می‌دهد. حداقل طول پسورد شما نباید کمتر از ۸ کاراکتر باشد.

۴- لازم است پسورد خود را به صورت دوره ای (هر سه ماه یکبار) تغییر دهید.

۵- هیچ‌گاه شناسه یا پسورد خود را در اختیار افراد دیگر قرار ندهید.

۶- هیچ‌گاه اطلاعات حساب و کارت بانکی خود را از طریق پیامک برای دیگران ارسال ننمایید. درصورتیکه شماره‌حساب یا شماره‌کارت شما به همراه هریک از اطلاعات ذیل در اختیار افراد غیرمجاز قرار گیرد، امنیت حساب شما در معرض خطر قرار می‌گیرد :

a. رمزهای اول و دوم

b. شماره CVV2

c. تاریخ انقضای کارت

۷- در صورتیکه فکر می‌کنید اطلاعات شخصی (شناسه یا پسورد) شما افشا شده است سریعاً با شماره بانک مربوطه تماس بگیرید.

۸- نگهداری رمز در نزدیکی کارت بانکی و یا داخل هرگونه محافظ کنار کارت صحیح نمی‌باشد زیرا در صورت سرقت یا مفقود شدن هر یک از وسایل مذکور ، سارق امکان سوءاستفاده از حساب را براحتی خواهد داشت.

۹- هنگام وارد نمودن رمز اینترنت بانک حتماً از صفحه کلید امنیتی استفاده کنید. برخی برنامه‌های جاسوسی، داده‌های وارد شده توسط صفحه کلید شما را کنترل می‌کنند.

۱۰- هنگام واردکردن رمز ، مستقیماً جلوی دستگاه قرار بگیرید تا کسانی که در انتظار استفاده از دستگاه‌خودپرداز می‌باشند، متوجه رمز شما نشوند. همچنین درصورت امکان در هنگام وارد نمودن رمز، دست دیگر خود را بصورت حایل روی صفحه اعداد قرار دهید.

v نکات مربوط به کامپیوتر مورد استفاده در زمان اتصال به سایت بانک

۱- برای جلوگیری از دسترسی غیرمجاز به کامپیوتر شخصی خود از فایروال استفاده کنید.

۲- نرم افزار آنتی ویروس را روی سیستم خود نصب کنید و آن را به روز نگهدارید.

۳- ایمیل‌های حاوی پیوست که از منابع ناشناس به شما ارسال شده را بدون بازکردن، پاک کنید.

۴- اطمینان حاصل کنید که هنگام وارد کردن شناسه کاربری و پسورد، شخص دیگری صفحه کلید شما را مشاهده نمی‌کند.

۵- مادامی که از سامانه بانک اینترنتی خود خارج نشده‌اید، کامپیوتر خود را ترک نکنید. بعد از اتمام کار خود حتما از سامانه خارج شوید (Logout کنید).

۶- هیچ‌گاه اطلاعات شخصی خود از قبیل پسورد اینترنت بانک را از طریق ایمیل ارسال نکنید.

۷- هیچ بانکی نیاز به اطلاعات محرمانه حساب شما (به خصوص پسورد شما) ندارد. به ایمیل‌هایی که به عنوان بانک این اطلاعات را از شما می‌خواهند توجه نکنید.

۸- هرگز از طریق کامپیوترهای عمومی (مانند کافی‌نت ها)، کامپیوتر افراد ناشناس و هر سیستمی که به امن بودن آن اطمینان ندارید، از خدمات بانکی الکترونیکی استفاده نکنید.

۹- هیچ گاه در رایانه‌ای که با آن به اینترنت بانک وارد می شوید، به سایت های نامطمئن وارد نشوید و ایمیل های مشکوک را باز نکنید. این سایت‌ها یا ایمیل‌ها می‌توانند نرم افزارهای جاسوسی را بدون اجازه و مخفیانه روی رایانه شما نصب نمایند.

v نکات مربوط به مرورگر وب

۱- اطمینان حاصل کنید که به وب سایت بانک متصل هستید (از طریق آدرس درج شده در بخش URL مرورگر) ، نه به سایتی که صرفاً شباهت ظاهری به آن دارد.

۲- از وجود علامت قفل طلایی رنگی که در کنار آدرس سایت یا در پایین صفحه مرورگر قرار دارد و از HTTPS بودن ابتدای آدرس اطمینان حاصل کنید، در غیر اینصورت پسورد خود را وارد نکنید.

۳- اگر پیغامی به زبان انگلیسی مبنی بر نامعتبر بودن گواهی سایت یا عدم برقراری اتصال امن مشاهده کردید، پسورد خود را وارد نکنید.

۴- هرگز به تقاضاهایی که از طریق ایمیل یا پنجره‌های pop-up اطلاعات شخصی شما را می‌خواهند، پاسخ ندهید.

v نکات مربوط به دستگاه‌های خودپرداز و POSهای فروشگاهی

۱- در زمان استفاده از پایانه‌های فروشگاهی POS رمز عبور کارت را خودتان وارد کنید.

۲- در هنگام وارد کردن رمز عبور در دستگاه‌های POS فروشگاهی و یا خودپردازها مواظب باشید تا رمز عبورتان را دیگران نبینند.

۳- در صورت مشاهده هر گونه تغییر در دستگاه ATM و یا مشاهده موارد مشکوک (تغییر در کارت‌خوان، تغییر صفحه‌کلید و یا دوربین نصب شده مشکوک) از دستگاه استفاده نکرده و سریعاً آن را به مسئول شعبه اطلاع دهید.

۴- با توجه به اینکه در رسیدهای دریافتی از دستگاه خودپرداز اطلاعات حساب شما از جمله شماره حساب و موجودی درج می‌شود، رسیدهای دریافتی را حتی المقدور تا عملیات بعدی نزد خودتان نگهداری نموده و در غیر اینصورت در محل‌هایی که به منظور جمع آوری رسیدهای مورد نظر تعبیه گردیده قرار دهید و از رها نمودن آنها در اطراف دستگاه‌های خودپرداز خودداری نمایید.