



# آنچه توانسته ایم لطف خدا بوده است

## توصیه های امنیتی به مشتریان پایانه های فروش (POS)

- قبل از خرید از طریق پایانه های فروش موجود در فروشگاه ها ، برای مانده گیری کارت خود از طریق همان کارت خوان فروشگاه اقدام کنید تا در صورت تراکنش خرید ناموفق در فروشگاه امکان اثبات مانده به فروشنده باشد.
- در فروشگاه ها و هنگام خرید از پایانه فروش، خودتان رمز کارت را وارد دستگاه کنید و از اعلام آن به فروشنده خودداری نمایید.
- هنگام وارد نمودن رمز کارت در پایانه فروش ، می توان دست دیگر را به عنوان محافظ انگشتان وارد کننده رمز قرار داد تا امکان مشاهده رمز برای دیگران وجود نداشته باشد.
- در صورتیکه در فروشگاهی مجبور به اعلام رمز کارت خود شدید، در اولین فرصت نسبت به تغییر رمز کارت خود اقدام نمایید.
- در صورت اجبار ارائه رمز به مسئول فروشگاه، رمز خود را از طریق صفحه موبایل یا روی کاغذ نوشته و نشان وی دهید و بلافاصله آن را پاک کنید و از وارد نمودن رمز توسط مسئول فروشگاه در پایانه فروش اطمینان حاصل نمایید.
- از پایانه فروش صرفاً برای خرید، مانده گیری و پرداخت قبض استفاده نمایید.
- دستگاه های پایانه فروش امکان واریز یا انتقال وجه به حساب خود یا دیگران را به شما نمی دهند، لذا چنانچه این امکان را روی پایانه فروشی مشاهده نمودید هرگز از آن استفاده نکنید.
- رسید تراکنش ناموفق خود را تا اطمینان از کسر نشدن وجه از حسابتان نگهداری کنید.
- پذیرندگان پایانه های فروش دقت نمایند، ماموران تعمیر دستگاه پایانه فروش دارای کارت شناسایی از شرکت مربوطه خود می باشند، ضمن اخذ آن از سپردن دستگاه خود به افراد ناشناس خودداری کنید.

## توصیه های امنیتی به مشتریان استفاده کننده از همراه بانک (MOBILE BANK)

- نرم افزار همراه بانک را مستقیماً از روی سایت اختصاصی بانک مربوطه دریافت کنید و هرگز از سایت های غیرمعتبر و پست الکترونیکی دریافت را انجام ندهید.
- به هیچ وجه رمز های مربوطه شامل: رمز حساب، رمز اول و دوم کارت و رمز ورود به نرم افزار همراه بانک را در اختیار دیگران قرار ندهید و آنها را در فواصل زمانی تغییر دهید.
- در صورت مفقود شدن یا سرقت گوشی یا سیم کارت تلفن همراه خود، بلافاصله رمز حساب و رمز دوم کارت خود را تغییر دهید.
- برای افزایش ضریب امنیت و کارایی سیستم همراه بانک، به صورت دوره ای از طریق گزینه بازگشت به تنظیم اولیه، تنظیم برنامه را به حالت اول برگردانید.

- پیام های دریافتی از این سیستم که در منوی صندوق پیام های برنامه قرار می گیرند را پس از خواندن، حذف نمائید.
- پیش از واگذاری گوشی تلفن همراه خود به دیگران، ابتدا گزینه بازگشت به تنظیم های اولیه را انتخاب و برنامه را از روی گوشی حذف کنید با این اقدام همه اطلاعات حساب های ثبت شده و نیز پیام های دریافتی شما بر روی گوشی از بین خواهد رفت.
- پیش از واگذاری سیم کارت، چنانچه سیم کارت دیگری را جایگزین نمی کنید لازم است حساب ها و سرویس های یک طرفه درخواستی خود را حذف کنید و در صورتی که از سیم کارت جایگزین استفاده می نمائید، لازم است پس از تعویض سیم کارت ابتدا گزینه بازگشت به تنظیمات اولیه را انتخاب نموده و با استفاده از گزینه های انتقال حساب ها به سیم کارت فعلی و انتقال سرویس ها به سیم کارت فعلی، ثبت نام حساب ها و سرویس های یک طرفه خود را به سیم کارت جدید انتقال دهید.

### **توصیه های امنیتی جهت جلوگیری از کلاهبرداری در هنگام استفاده از خودپرداز ها(ATM)**

- جهت انتقال وجه تنها اعلام شماره حساب و یا شماره کارت به فرد انتقال دهنده (واریز کننده) کفایت می کند و نیازی به گفتن رمز اول، دوم، CVV2، تاریخ انقضاء و غیره نیست.
- برای اطمینان از واریز وجه، نیازی به ورود به بخش انتقال وجه نیست و دارنده کارت فقط با گرفتن موجودی حساب خود می تواند از واریز شدن یا واریز نشدن وجه به حساب و کارت خود مطلع شود.
- کارت بانکی خود را در اختیار افراد ناشناس قرار ندهید و در صورت مفقودی یا سرقت در اسرع وقت با بانک صادرکننده کارت تماس گرفته و یا از طریق اینترنت بانک و تلفن بانک یا مراجعه مستقیم به یکی از شعبه های بانک مربوطه نسبت به مسدود نمودن و باطل کردن کارت خود به منظور جلوگیری از هرگونه سوءاستفاده اقدام نمائید.
- اگر افراد ناشناس تقاضای استفاده از خدمات بانکی بوسیله کارت شما را داشتند، آن را نپذیرید و هنگام استفاده از خدمات بانکی بوسیله کارت دقت نمائید مشخصات و جزئیات کارت برای دیگران قابل مشاهده نباشد.
- از کارت بانکی خود صرفاً برای انجام مبادلات خرد (مبالغ کم) استفاده کنید و از متصل نمودن حساب هائی که گردش مالی زیاد دارند، به کارت خود اجتناب نمائید.
- از نبود دوربین سارقان در محیط اطراف خودپرداز اطمینان حاصل کنید ( دوربین های کوچکی که کمتر قابل مشاهده می باشند و برای رویت رمز کارت بانکی مشتریان در اطراف خودپرداز و با حداقل فاصله با صفحه کلید خودپرداز نصب می شوند).
- در صورت ضبط کارت توسط خودپرداز دقت نمائید که حداقل یکی از موارد ذیل می بایست رخ دهد: نمایش پیام خارج از سرویس شدن خودپرداز، چشمک زدن چراخ LED کارت خوان و ارائه رسید توسط خودپرداز، در غیر این صورت تا حصول اطمینان از ضبط کارت و یا بیرون آمدن کارت از دستگاه محل خودپرداز را ترک نکنید.
- برای انتقال وجه از طریق خودپرداز نیازی به استفاده از منوی انگلیسی نیست. منوی انگلیسی صرفاً برای استفاده مسافران خارجی تعبیه شده است. مراقب باشید فقط کلاهبرداران، شما را به استفاده از منوی انگلیسی خودپرداز تشویق و وانمود می کنند که برای انتقال وجه، باید از کارت ارزی خود استفاده و شما را ترغیب به استفاده از منوی انگلیسی می کنند.

### توصیه های امنیتی به مشتریان خرید آنلاین کالاها و خدمات (خرید اینترنتی)

- اولین پیش فرض برای حقیقی و سالم بودن خدمات یک فروشگاه الکترونیک، این است که کالا های مجاز ارائه می نمایند. بنابراین فروشگاه هایی که کالاهای غیرمجاز به فروش می رسانند، با احتمال بسیار بالا به قصد کلاهبرداری ایجاد شده اند .
- در هنگام تصمیم به خرید از فروشگاه های الکترونیکی، از تجربه دوستان و آشنایان نزدیک در خصوص خرید های آنلاین استفاده کنید و از فروشگاه هایی که سابقه ارائه خدمات مطلوب دارند، خرید کنید.
- صفحاتی که ناخواسته در برابر شما باز می شوند و حاوی تبلیغات فروش کالاها و ارائه خدمات هستند، ممکن است تقلبی بوده و قصد کلاهبرداری داشته باشند.
- سعی کنید در هنگام خرید آنلاین، با روش هایی نظیر گرفتن WHO IS از دامنه سایت اینترنتی فروشگاه یا جستجو در انجمن هایی که اعضای آنها، تجربیات خرید آنلاین خود را برای اطلاع سایر اعضا می نویسند، از مدیر و گردانندگان فروشگاه، احراز هویت کنید.
- در هنگام خرید آنلاین و در زمانی که پس از انتخاب کالا به درگاه پرداخت الکترونیکی بانک رهنمون می شوید، دقت کنید که حتما آدرس صفحه درگاه پرداخت الکترونیکی، متعلق به همان بانک باشد که آرم و لوگوی آن را در صفحه مشاهده می کنید.
- در بعضی مواقع کلاهبرداران با جعل صفحات درگاه پرداخت الکترونیکی بانک ها، شما را به صفحاتی هدایت می کنند که آدرسی بسیار شبیه آدرس بانک اصلی دارند. در صورت عدم دقت خریدار و ورود اطلاعات کارت بانکی خود شامل شماره کارت، رمزعبور ، CVV2 و تاریخ انقضای کارت، این اطلاعات را در سیستم خود ثبت کرده و عملا امکان هرگونه اقدامی را با حساب و موجودی قربانی دارند.
- سیستم پرداخت الکترونیکی همه بانک ها از SSL و روش های مطمئن رمزنگاری استفاده می کنند. دقت نمائید که در نوار آدرس اینترنتی صفحه پرداخت بانک، نماد یک قفل با عبارت HTTPS:// درج شده باشد. در غیر این صورت قطعا صفحه جعلی بوده و قصد به سرقت بردن اطلاعات کارت بانکی شما را دارد.

### توصیه های امنیتی به مشتریان حساب بانکی

- هیچ وقت اطلاعات محرمانه کارت خود نظیر رمز اول یا دوم، CVV2 و تاریخ انقضای کارت را در جایی یادداشت نکرده و از ارائه آن به سایر افراد به شدت خودداری کنید.
- از رمزهایی استفاده کنید که حداقل شامل ۸ کارکتر باشد و حداکثر هر ۶۰ روز یک بار رمز عبور خود را تغییر دهید.
- هنگام برداشت وجه از خودپرداز بانک ها مراقب باشید افراد سود جو رمز کارت بانک شما را مشاهده نکنند.
- کارت های بانک غیر ضروری به همراه نداشته باشید و موجودی بانکی خصوصا حساب های متصل به کارت را در فاصله زمانی مناسب کنترل کنید.

- برکه رسیدی که از خودپرداز یا پایانه فروش دریافت می کنید را در محل رها نکرده و در صورت عدم نیاز آن را معدوم نمائید.
- از ارائه اطلاعات مالی و بانکی خود از قبیل شماره حساب، شماره کارت های اعتباری و اعلام رمز آنها و غیره به سایت های متفرقه و مشکوک خودداری کنید و از عملکرد اینترنتی و قانونی بانک ها و سایر مراکز دولتی و رسمی اطمینان حاصل کنید.
- در هنگام استفاده از امکانات اینترنتی بانک ها و موسسات مالی یا خرید های اینترنتی از ذخیره کردن نام کاربری و رمز عبور در رایانه خودداری کنید.
- با توجه به اینکه کلاهبرداران اینترنتی برای بدست آوردن اطلاعات حساب های بانکی افراد در سایت های اینترنتی بانک ها، اقدام به ایجاد و راه اندازی سایت های مشابه سایت بانکی می کنند لذا در صورت اتصال به این سایت ها از اصلی بودن آن مطمئن شوید.
- همیشه به یاد داشته باشید هیچ بانک یا نهاد دولتی، اطلاعات محرمانه حساب شما را به صورت تلفنی و یا با پیامک از شما درخواست نمی کند. در صورت برخورد با چنین مواردی از ارسال اطلاعات خودداری و مراتب را به مسئولان بانک مربوطه اطلاع دهید.

## **" نکات قابل توجه در بهره برداری از خدمات بانکداری الکترونیک "**

۱. هنگام دریافت پاکت رمز کارت بانک خود از شعبه، به سلامت و عدم پارگی پاکت دقت نمایید.
۲. به محض وصول رمز کارت صادره، به دستگاه خودپرداز مراجعه کرده و رمز خود را تغییر دهید.
۳. به محض دریافت کارت بانک، نسبت به یادداشت کردن شماره ۱۶ رقمی آن اقدام نمایید. به خاطر داشته باشید برای مسدود کردن حساب، هنگام سرقت یا مفقود شدن کارت به این شماره نیاز دارید.
۴. شماره چهار رقمی که به عنوان رمز استفاده می کنید، به سادگی برای دیگران قابل حدس زدن نباشد. برای مثال از سال تولد، سال ازدواج یا شماره تلفن خود استفاده نکنید.
۵. فقط کلاهبرداران وانمود می کنند که برای انتقال وجه، می بایست از کارت ارزی خود استفاده کنند و شما را ترغیب به استفاده از منوی انگلیسی می نمایند.
۶. برای انتقال وجه، نیازی به استفاده از منوی انگلیسی نیست. منوی انگلیسی برای بهره برداری مسافران خارجی ایجاد شده است.
۷. مراقب باشید: فقط کلاهبرداران شما را به استفاده از منوی انگلیسی ترغیب می نمایند.

۸. هنگام انجام عملیات انتقال وجه، فرد دریافت کننده فقط شماره ۱۶ رقمی کارت خود را اعلام می کند و نیازی به ارائه سایر اطلاعات کارت یا مراجعه به دستگاه خودپرداز ندارد.
۹. رمز جدید را به خاطر بسپارید، از یادداشت کردن رمز کنار کارت و قرار دادن برگه رمز در کیف کارت جداً خودداری فرمایید.
۱۰. هنگام وارد کردن رمز در دستگاه خودپرداز، به گونه ای جلوی دستگاه بایستید که کسی امکان دیدن صفحه کلید و رمز شما را نداشته باشد.
۱۱. رمز خود را هر سه تا چهار ماه تغییر دهید.
۱۲. در فروشگاهها و هنگام خرید از پایانه فروش، خودتان رمز را وارد دستگاه کنید و از اعلام آن به فروشنده خودداری نمایید.
۱۳. در صورتیکه در فروشگاههای مجبور به اعلام رمزتان شدید، حتی المقدور به سرعت نسبت به تغییر رمز خود اقدام نمایید.
۱۴. از سپردن کارت خود به دیگران خودداری نمایید. در صورت لزوم، بلافاصله نسبت به تغییر رمز خود اقدام نمایید.
۱۵. رسید دریافتی از دستگاه خودپرداز و کارتخوان را در محل رها نکنید.
۱۶. در صورت بروز اشکال در عملیات بانکی، از توسل به افراد غریبه جداً خودداری نمایید.
۱۷. از پایانه فروش فقط برای خرید، مانده گیری و پرداخت قبض استفاده کنید.
۱۸. برای انتقال وجه به سایر حساب های خود یا دیگران به هیچ وجه از پایانه فروش استفاده نکنید.
۱۹. برای انتقال وجه از دستگاه های خودپرداز، پایانه شعبه ها یا خدمات ساتنا و پایا که در داخل شعبه ارائه می شود، بهره برداری نمایید.
۲۰. سقف انتقال وجه دستگاه خودپرداز سه میلیون تومان در هر روز می باشد.
۲۱. با مراجعه به شعبه و استفاده از پایانه شعبه می توانید تا سقف پانزده میلیون تومان به صورت آنی به سایر کارت های خود یا دیگران انتقال وجه دهید.
۲۲. با مراجعه به شعبه و استفاده از سامانه پایا می توانید به هر حسابی در هر بانک تا سقف پانزده میلیون تومان در همان روز انتقال وجه دهید.

۲۳. با مراجعه به شعبه و استفاده از سامانه ساتنا می توانید به هر حسابی در هر بانک به صورت نامحدود در همان روز انتقال وجه دهید.
۲۴. برای انجام عملیات انتقال وجه از طریق پایا و ساتنا دانستن شماره شبای حساب مقصد الزامی است.
۲۵. یک راه اطلاع از شماره شبا، مراجعه به شعبه یا سایت افتتاح کننده حساب است.
۲۶. هرگز برای دریافت شماره شبای بانک "الف" به سایت بانک "ب" مراجعه ننمایید.
۲۷. بانک مسئولیتی برای جبران خسارت مشتریانی که شماره شبای مقصد را اشتباه ثبت کرده اند، نخواهد داشت.
۲۸. با داشتن کارت بانک می توانید قبوض خود را بدون مراجعه به شعبه های بانک ها پرداخت نمایید.
۲۹. مراجعه به دستگاه خودپرداز هر یک از بانک ها یک راه پرداخت سریع قبض شماست.
۳۰. مراجعه به پایانه فروش نصب شده در فروشگاه محل سکونت شما، یک راه پرداخت سریع قبض شماست.
۳۱. مراجعه به پایانه شعبه هر یک از بانک ها یک راه پرداخت سریع قبض شماست.
۳۲. مراجعه به سایت هر یک از بانک ها یک راه پرداخت سریع قبض شماست.
۳۳. برای خریدهای اینترنتی داشتن رمز دوم الزامی است.
۳۴. برای دریافت رمز دوم کارت به دستگاه خودپرداز بانک خود مراجعه کنید.
۳۵. رمز اول و دوم کارت شما محرمانه است. از ارائه اطلاعات محرمانه کارت خود به دیگران خودداری نمایید.
۳۶. کد CVV2 کارت شما محرمانه است. از ارائه اطلاعات محرمانه کارت خود به دیگران خودداری نمایید.
۳۷. به محض اطلاع از مفقود شدن کارت خود، نسبت به مسدود کردن آن اقدام نمایید.
۳۸. به محض اطلاع از به سرقت رفتن کارت خود، نسبت به مسدود کردن آن اقدام نمایید.
۳۹. یک راه مسدود کردن کارت بانک، مراجعه به شعبه های بانک صادر کننده کارت است.
۴۰. یک راه مسدود کردن کارت بانک، مراجعه به سایت اینترنتی بانک صادر کننده کارت است.
۴۱. یک راه مسدود کردن کارت بانک، تماس با میز امداد بانک صادر کننده کارت است.
۴۲. برای مسدود کردن کارت بانک داشتن رمز دوم کارت الزامی است.
۴۳. هرگز برای پر کردن حساب جاری از پایانه فروش استفاده نکنید.
۴۴. انتقال وجه از طریق اینترنت بانک، فقط با داشتن رمز مخصوص اینترنت بانک امکان پذیر می باشد.
۴۵. برای انجام عملیات انتقال وجه شتابی از همراه بانک استفاده ننمایید.

۴۶. در صورت عدم پرداخت اقساط کارت های اعتباری، کارت اعتباری شما به مدت شش ماه مسدود خواهد شد.
۴۷. برای بهره برداری موثر از خدمات بانکداری الکترونیکی و ایمن ماندن از ریسک های احتمالی، هنگام افتتاح حساب و درخواست کارت بانک، بروشورهای مربوطه را به دقت مطالعه فرمایید.
۴۸. سایت بانک ها منبع مفیدی برای دریافت نکات ایمنی هنگام بهره برداری از خدمات بانکداری الکترونیکی است.
۴۹. سایت پلیس فتا [www.cyberpolice.ir](http://www.cyberpolice.ir) منبع مفیدی برای دریافت آخرین اطلاعات مربوط به تهدیدات امنیتی است.
۵۰. شماره تلفن ۲۹۹۱۱ راهی آسان برای ثبت مغایرت های شماست.
۵۱. مامورین تعمیر پایانه فروش شرکت شما دارای کارت شناسایی از شرکت مربوطه هستند. از سپردن دستگاه خود به افراد ناشناس خودداری نمایید.
۵۲. رسید تراکنش های ناموفق خود را تا حصول اطمینان از کسر نشدن وجه از حسابتان نگهداری نمایید.
۵۳. استفاده از صفحه کلید مجازی سایت راهی مطمئن برای وارد کردن رمز می باشد.
۵۴. هنگام انجام خرید یا پرداخت قبض در اینترنت، حتماً از صفحه کلید مجازی برای وارد کردن رمز خود استفاده نمایید.
۵۵. شبها از مراجعه به خودپردازهایی که در محل های کم رفت و آمد و تاریک قرار دارند، خودداری نمایید.
۵۶. توجه داشته باشید آدرس سایت سیستم اینترنت بانک و یا پرداخت اینترنتی در مرورگر باید با **https** آغاز شود.
۵۷. برای ورود به سیستم اینترنت بانک و یا پرداخت اینترنتی هرگز از مکان های عمومی مانند کافی نت ها استفاده نکنید.
۵۸. در انتخاب نام کاربری و کلمه عبور خود دقت نمایید تا دیگران نتوانند آن را حدس بزنند.
۵۹. بدون خروج قطعی از اینترنت بانک، کامپیوتر را ترک نکنید.
۶۰. با وارد کردن آدرس پست الکترونیکی هنگام پرداخت قبض یا خرید اینترنتی، بانک رسید عملیات را برای شما ارسال می نماید که برای اطلاع و بهره برداری آتی بسیار مفید خواهد بود.
۶۱. از انجام پرداخت های اینترنتی از طریق سایت های متعلق به موسسات غیرمعتبر و ناشناس در اینترنت خودداری نمایید.

۶۲. هیچ بانکی به اطلاعات محرمانه کارت شما (نظیر رمز اول یا دوم، کد CVV2 و تاریخ انقضای کارت) نیاز ندارد. به ایمیل ها و پیامک هایی که به عنوان بانک این اطلاعات را از شما می خواهند، هرگز پاسخ ندهید.
۶۳. هرگز به تقاضاهایی که از طریق ایمیل یا پنجره های pop-up اطلاعات شخصی شما را می خواهند پاسخ ندهید.
۶۴. از کامپیوتر افراد ناشناس یا کافی نت ها برای انجام عملیات بانکی خود استفاده نکنید.
۶۵. روش های متعدد مسدودی کارت عبارتند از: اینترنت بانک، تلفن بانک، موبایل بانک، خودپرداز، شعبه، مرکز ارتباط با مشتریان. به نحوه مسدودی کارت در بانک صادر کننده کارت خود در ساعات کاری و ایام تعطیل توجه کنید.
۶۶. لطفاً به محض اطلاع از مفقودی یا سرقت کارت خود، حساب خود را مسدود نمایید.
۶۷. هنگام دریافت کارت خود از شعبه بانک، شماره ۱۶ رقمی کارت و شماره تماس خدمات مشتریان بانک را از پشت کارت برای موارد ضروری یادداشت فرمایید.
۶۸. برای دریافت رمز دوم به دستگاه خودپرداز بانک صادر کننده کارت خود مراجعه فرمایید.
۶۹. درخواست ارسال پیامک در انجام تراکنش ها و ورود به خدمات غیرحضوری مانند اینترنت بانک، تلفن بانک و... باعث آگاهی مشتری از سواستفاده احتمالی و جلوگیری از سواستفاده بیشتر می شود، به محض دریافت چنین پیامکی در صورتیکه خودتان تراکنشی انجام نداده اید، نسبت به تعویض رمز خود اقدام نمایید.