

• توصیه ها و آموزش های لازم به مشتریان در خصوص مخاطرات ناشی از ورود عوامل نفوذی،

آلودگی ویروسی، جعل هویت و موارد مشابه:

با پیشرفت تکنولوژی و ارائه خدمات به مشتریان بصورت دیجیتال از طریق فضای وب، همواره این فضا با چالش هایی اعم از سوء استفاده های مختلف توسط مجرمین و کلاهبرداران سایبری روبرو بوده است.

از چالش های موجود می توان به نشت اطلاعات و سوء استفاده توسط عوامل نفوذی، آلودگی ویروسی، جعل هویت و... اشاره نمود. عوامل نفوذی بصورت فیزیکی و مجازی قادر خواهند بود اطلاعات حیاتی، اطلاعات هویتی و شخصی افراد و... را به سرقت برده و از آن سوء استفاده نموده و یا ایجاد خرابکاری نمایند. لذا دقت لازم در این خصوص (از جمله رعایت موارد ذیل)، سبب پیشگیری از مخاطرات مربوطه خواهد گردید:

- ۱- هرگز از طریق تعقیب پیوند بانک در موتورهای جستجو و یا شبکه های اجتماعی به آن وارد نشوید و مستقیماً آدرس سایت رسمی بانک را وارد نمایید.
- ۲- در هنگام استفاده از درگاه های پرداخت در صورت هشدار عدم اعتبار گواهی از ادامه عملیات خودداری نمایید.
- ۳- از سایت هایی که اطلاعات مبادله شده بین شما و سرور را رمزنگاری می کنند مانند سایت هایی که آدرس آنها با *https* شروع می شوند استفاده کنید.
- ۴- برای پرداخت های اینترنتی حتماً از سایت هایی که به آنها اطمینان دارید استفاده کنید. برای مثال از علامت قفل موجود در سایت و نیز درج آدرس صحیح سایت، اطمینان حاصل نمایید.
- ۵- توصیه می شود از مرورگرهای مطمئن و به روز استفاده کنید.
- ۶- همواره از نرم افزارهای آنتی ویروس معتبر و به روز شده استفاده نمایید.
- ۷- توصیه میشود در زمان پرداخت از رمز یکبار مصرف و از صفحه کلید مجازی مربوطه استفاده نمایید.
- ۸- رمزهای عبور خود را در فواصل زمانی کوتاه تغییر دهید.
- ۹- بانک هرگز اطلاعات محرمانه شما را از طریق پست الکترونیکی یا تماس تلفنی و پیامک درخواست نمی کند. در صورت رخداد این موارد، سریعاً مراتب را به بانک اطلاع دهید.
- ۱۰- پس از اتمام عملیات بانکی حتماً از محیط اینترنت بانک خارج شوید. یک بار غفلت ممکن است مخاطره آمیز باشد.
- ۱۱- تنها راه صحیح نگهداری رمز به خاطر سپردن آن است. از نوشتن بر روی کاغذ یا بیان کردن آن هنگام وارد کردن رمز جداً خودداری کنید.
- ۱۲- به هر صفحه تبلیغاتی که در مرورگر درخواست باز شدن می دهد، اجازه باز شدن ندهید. (برخی برنامه های نا امن در قالب *pop-up* اجرا می شوند).
- ۱۳- همواره بر روی رایانه خود یک نرم افزار دیواره آتش داشته باشید.
- ۱۴- تاریخچه و کوکی های مرورگر خود را مرتباً پاک کنید.
- ۱۵- فایل های به روزرسانی و وصله های امنیتی سیستم عامل و نرم افزارهای کاربردی را به طور مرتب دریافت و نصب کنید.

- ۱۶- هر جایی که نیاز به تعریف نام کاربری و کلمه عبور دارید، از کلمات غیر قابل حدس، پیچیده به صورت ترکیبی از اعداد و حروف استفاده کرده و هرگز از کلمات و اعداد خاص مانند کد ملی، تاریخ تولد، شماره تلفن خود یا اعضای خانواده، شماره شناسنامه، اسامی پرکاربرد و ... استفاده نکنید.
- ۱۷- هنگام انجام عملیات بانکی در محیط اینترنت بانک با آرامش کامل و بدون دستپاچگی به عملیات بانکی خود بپردازید. زیرا اضطراب و عجله ممکن است موجب بروز خطای سنگین شود.
- ۱۸- از باز نمودن ایمیل های ناشناس و ضمیمه های آن و یا کلیک بر روی لینک های داخل متن ایمیل، جداً خودداری نمایید.
- ۱۹- ایمیل های مالی و یا شماره حسابهایی که قرار است به آن مبلغ واریز نمایید را به صورت تلفنی کنترل نمایید.
- ۲۰- آدرس ایمیل ها دریافتی را به صورت دقیق بررسی و استعلام نمایید.
- ۲۱- موقع دریافت کارت از بانک، از بسته بودن پاکت کارت خصوصاً رمز عبور اطمینان حاصل کنید.
- ۲۲- بلافاصله رمز عبور را پس از دریافت کارت از طریق یکی از دستگاه های خودپرداز تغییر دهید. سعی کنید رمز عبورتان را هر چند وقت یکبار تغییر دهید.
- ۲۳- هرگز رمز عبور خود را با کارت در یک محل نگهداری نکنید.
- ۲۴- در زمان استفاده از پایانه های فروشگاهی *POS* رمز عبور کارت را خودتان وارد کنید.
- ۲۵- در هنگام وارد کردن رمز عبور در دستگاه های *POS* فروشگاهی و یا خودپردازها مواظب باشید تا رمز عبورتان را دیگران نبینند.
- ۲۶- در هر سایتی مشخصات کارت خود را وارد نکنید ممکن است آن سایت یک دام باشد که صرفاً اقدام به دریافت رمز عبور شما می کند.
- ۲۷- کارت خود را حتی برای مدت کوتاه در اختیار کسی قرار ندهید ممکن است از روی آن کپی تهیه کنند و با بدست آوردن رمز عبور آن موجودی حساب شما را برداشت نمایند.
- ۲۸- حتماً شماره ۱۶ رقمی روی کارت و شماره حساب خود را در جایی یادداشت نمایید تا در زمان مفقودی کارت بلافاصله از طریق مراجعه به شعب، دستگاه خود پرداز، تلفن بانک یا ... اقدام به مسدود کردن کارت یا حساب خود نمایید.
- ۲۹- اگر در زمان مفقودی کارت شماره ۱۶ رقمی کارت خود را نداشتید، بلافاصله از طریق شعبه صادرکننده یا صدای سپهر کارت خود اقدام به مسدود کردن کارت یا حسابتان نمایید.
- ۳۰- کارت خود را نزدیک اشیاء مغناطیسی مانند آهن ربا، تلویزیون، تلفن همراه قرار ندهید تا عمر بیشتری داشته باشد.
- ۳۱- در صورت مشاهده هر گونه تغییر در ظاهر دستگاه خودپرداز و یا مشاهده موارد مشکوک (تغییر در دهانه ورودی کارت خوان، تغییر صفحه کلید و یا دوربین نصب شده مشکوک) از دستگاه استفاده نکرده و سریعاً آن را به مسئول شعبه اطلاع دهید.
- ۳۲- در صورتی که به عملیات بانکی از طریق کارت آشنایی ندارید به هیچ وجه از افراد ناشناس کمک نگیرید. زیرا ممکن است فرد ناشناس اقدام به عملیاتی غیر از عملیات موردنظر شما نماید. برای مثال می تواند علاوه بر پرداخت قبوض یا دریافت وجه برای شما، باقی مانده موجودیتان را به حساب خودش منتقل کند.
- ۳۳- سعی کنید حتی الامکان برای پرداخت های اینترنتی از کافی نت ها، وای فای رایگان در پمپ بنزین ها یا ایستگاه های حمل و نقل مانند فرودگاه ها و اماکن عمومی استفاده نکرده و از کامپیوتر شخصی خود یا تلفن همراهتان اقدام به پرداخت نمایید.

- ۳۴- کامپیوتری که بر روی آن آنتی ویروس وجود ندارد را برای پرداخت اینترنتی انتخاب نکنید.
- ۳۵- دستگاه هایی شبیه *pos* هستند که عملاً ماهیت یک *Reader* را داشته و صاحب فروشگاه با کشیدن کارت بر روی دستگاه فوق تمام اطلاعات اعم از شماره کارت را شناسایی و ضبط می نماید تا بعداً با کپی کارت از آن سوء استفاده و موجودی کارت را خارج نمایند. پس مراقب باشید.
- ۳۶- هنگام وارد نمودن رمز یا کدها حتماً از صفحه کلید امنیتی استفاده کنید. برخی برنامه های مخرب وجود دارند که داده های وارد شده توسط صفحه کلید رایانه شما را کنترل می کنند.
- ۳۷- کارت و رمز عبور خود را برای دریافت پول در اختیار افراد ناشناس قرار ندهید و هنگام برداشت وجه مواظب باشید کسی رمز شما را نبیند ضمن اینکه برگ رسیدی که از دستگاه خودپرداز دریافت می کنید را در محل رها نکنید و در صورتی که به آن نیاز ندارید برگه را معدوم کنید.
- ۳۸- موجودی حساب های بانکی را در فاصله های زمانی مناسب چک کنید و از ارائه اطلاعات مالی و بانکی خود از قبیل شماره حساب، شماره کارت های اعتباری و اعلام رمز آنها و ... به سایت های متفرقه و مشکوک بپرهیزید و از صحت عملکرد اینترنت بانک ها و سایر مراکز اطمینان حاصل کنید.
- ۳۹- از کارت بانکی خود کاملاً حفاظت و اگر آن را لازم ندارید حتماً با اطلاع بانک آن را باطل نمایید. کارت را رها نکنید و اگر رها کردید رمز آن را به هیچ وجه فاش نکنید چون مسئولیت هر نوع استفاده خلاف از کارت بانکی بر عهده کسی است که کارت به نامش صادر شده است.
- ۴۰- در فروشگاه هایی که امکان خرید با استفاده از کارت وجود دارد از دادن رمز کارت به فروشنده خودداری کنید.
- ۴۱- به هنگام حمل و نقل وجوه نقد با خودرو درب های اتومبیل را قفل کنید.
- ۴۲- سعی کنید حتی الامکان از حمل وجوه نقد، خودداری نموده و از سایر روشهای ممکن استفاده نمایید.
- ۴۳- اموال خود را از قبیل تلفن همراه، وجه نقد و غیره را در بانک در معرض دید قرار ندهید.
- ۴۴- به هنگام ورود و خروج از بانک کیفیتان را نزدیک بدنتان نگه دارید و اطمینان حاصل کنید که با امنیت کامل و محکم آن را نگه داشته اید.
- ۴۵- بند کیفیتان را دور گردن و یا مچ دست نیندازید ممکن است بر اثر قاپیدن آن با زور به شما آسیب وارد شود و خدای ناکرده اگر کیفیتان قاپیده شد آن را رها کنید تا مورد حمله قرار نگیرید یا به دنبال کیف کشیده نشوید.
- ۴۶- به هنگام خرید از فروشگاه کیف خود را در داخل سبد یا روی پیشخوان رها نکنید.
- ۴۷- در بانک و هنگام انتظار برای مراجعه به باجه، کیفیتان را به پشت صندلی آویزان نکنید.
- ۴۸- هیچ گاه از افراد ناشناس که معروفیت و اعتبار کافی ندارند چک، ایران چک، چک تضمینی و چک های بانکی قبول نکنید زیرا احتمال دارد آن چک ها مسروقه یا جعلی باشند.
- ۴۹- از گذاشتن و حمل کارت های بانکی غیر ضروری، اسناد، اوراق بهادار، دسته چک و اشیای گرانبها در کیفیتان در موارد غیر ضروری بپرهیز نمایید.
- ۵۰- به هنگام حمل وجه نقد یا اشیا و اسناد گرانبها به بانک از دیگر دوستان و اقوام مورد اطمینان خود کمک بگیرید.
- ۵۱- اگر قصد واریز یا برداشت پول از بانک را دارید که لازم است پول نقد و امثالهم حمل نمایید موضوع را با افراد غیر مطمئن بازگو نکنید.

- ۵۲- در صورتی که پول نقد حمل می کنید آن را در جیب بیرونی یا رو به بیرون خود نگذارید. چنانچه در کیف خود وجوه نقد دارید آن را به نمایش نگذارید چه بسا افرادی که در کنار شما به عنوان مشتری هستند با دیدن آن وسوسه شوند و پس از خارج شدن تان از بانک اقدام به قاپیدن و سرقت آن کنند.
- ۵۳- در داخل بانک ها از رهاکردن وجوه نقد خود روی پیشخوان بانک خودداری کنید.
- ۵۴- چنانچه پس از خروج از بانک مجبورید از وسایل نقلیه عمومی استفاده کنید؛ اتومبیل مطمئن مثلاً تاکسی سوار شوید و سوار مسافرهای شخصی غیر مطمئن نشوید.
- ۵۵- حتی المقدور برای جلوگیری از حمل وجه نقد زیاد از کارت های بانکی استفاده شود.
- ۵۶- از به نمایش گذاشتن وجه و شمردن آن در انظار عمومی که موجب تحریک سارقان می شود، خودداری کنید.
- ۵۷- برای انجام عملیات انتقال وجه از طریق پایا و ساتنا دانستن شماره شبای حساب مقصد الزامی است و یک راه اطلاع از شماره شبا، مراجعه به شعبه یا سایت اینترنتی بانک افتتاح کننده حساب است.
- ۵۸- بانک مسوولیتی برای جبران خسارت مشتریانی که شماره شبای مقصد را اشتباه ثبت کرده اند، نخواهد داشت.
- ۵۹- کد CVV2 کارت شما محرمانه است. از ارایه اطلاعات محرمانه کارت خود به دیگران خودداری کنید.
- ۶۰- ممکن است تماس تلفنی و یا دریافت پیامک مبنی بر « برنده شدن در قرعه کشی » کلاهبرداری باشد، لذا در صورت مواجهه با این موارد، مراتب صحت آن را از سازمان مربوطه استعلام نمایید.
- ۶۱- از قبول درخواست تلفنی و یا حضوری افراد ناشناس در خصوص هرگونه عملیات بانکی از جمله انتقال وجه، کارت به کارت و ارائه رمز اول و دوم کارت بانکی و ... اکیداً خودداری نمایید.
- ۶۲- انتخاب زبان انگلیسی برای انتقال وجه، مخصوص افراد غیر ایرانی می باشد، لذا جهت اطمینان از صحت انجام عملیات بانکی خود از منوی فارسی استفاده نمایید.
- ۶۳- اگر قرار است وجهی به حساب شما واریز و یا انتقال یابد، لازم نیست به دستگاه خودپرداز مراجعه نمایید.
- ۶۴- از ارائه کارت بانکی خود و رمز آن به افراد ناشناس جهت دریافت وجه (به لحاظ پیشگیری از سوء استفاده) خودداری نمایید.