
بانک خاورمیانه
Middle East Bank
پیشگیری از کلاهبرداری
4221
4221

برای این که بتوانید با سرعت و سهولت عملیات بانکی خود را انجام دهید بدون نیاز به حضور درشعبه، بدون نیاز به صرف زمان زیاد، استفاده از اینترنت بانک راه کار خوبی است. بانک خاورمیانه بخش قابل توجهی از نیازها، درخواست‌ها و تقاضاهای مشتریان را از کانال‌های الکترونیکی دریافت و پذیرش نموده و بخش قابل توجهی از خدمات خود را از این مسیر به مشتریان ارایه می‌نماید. در حال حاضر بانک خاورمیانه از طریق این سرویس خدمات سپرده، کارت، تسهیلات و چک را ارایه می‌نماید. هنگام انجام تراکنشهای مالی و خرید اینترنتی باید امنیت کامل را رعایت کنیم که در ادامه نکات امنیتی برای کاربران اینترنتی ارایه شده است.

نکات امنیتی برای خدمات حضوری

اطمینان از خاتمه عملیات بانکی

قبل از اطمینان از اتمام پردازش و خاتمه عملیات بانکی محل را ترک نکنید و در صورت بروز تراکنش ناموفق رسید مربوطه را تا حصول اطمینان از کسر نشدن وجه از حساب، نزد خود نگه دارید.

دریافت رسید

رسید دریافتی از دستگاه خودپرداز و کارت‌خوان را در محل رها نکنید.

حفظ امنیت در وارد نمودن رمز

در مکان‌های عمومی برای محافظت از اطلاعات محرمانه، هنگام استفاده از کارت و وارد نمودن رمز عبور در دستگاه خودپرداز (ATM) یا کارت‌خوان (POS)، با استفاده از دست دیگر خود یک سپر حفاظتی ایجاد کنید. این موضوع با هیچ یک از هنجارهای اجتماعی منافاتی نداشته و رعایت آن حافظ امنیت عملیات بانکی افراد خواهد بود.

خودداری از ارایه رمز کارت به فروشنده

در فروشگاه‌هایی که امکان خرید با استفاده از کارت بانکی وجود دارد از ارایه رمز عبور به فروشنده خودداری شده و شخصا رمز خود را در دستگاه کارت‌خوان وارد نمائید. در این خصوص فروشگاه ملزم به همکاری با مشتری بوده و حق اعتراض برای مشتریان محفوظ است.

رعایت فاصله در زمان استفاده از خودپرداز

در زمان استفاده از دستگاه خودپرداز دقت شود که فاصله مناسب نفر بعدی با شما رعایت شده باشد. انجام این نکته نشانه رعایت حقوق شهروندی و به تبع آن افزایش امنیت استفاده‌کننده از دستگاه خودپرداز است.

توجه به وضعیت خود پرداز

درصورت مشاهده وضعیت غیرعادی روی دریچه ورودی کارت یا خروجی وجه دستگاه خودپرداز (چسب خوردن، وجود شیء اضافه)، ضمن اعلام مراتب به مسئولین شعبه در ساعات کاری و کشیک شبانه‌روزی بانک در سایر ساعات شبانه روز، برای دریافت خدمت مورد نظر، از دستگاه خودپرداز دیگری استفاده شود.

کنترل وجه دریافتی

توصیه می‌شود پس از دریافت کارت و وجه مورد نیاز از دستگاه خودپرداز، در مکانی امن و مناسب، وجه دریافتی شمارش و کنترل شود.

اطمینان از واقعی بودن دستگاه خودپرداز

هنگام استفاده از دستگاه خودپرداز (ATM) یا دستگاه کارتخوان (POS) متصل به شاپرک حتی‌الامکان از واقعی بودن ابزار مزبور اطمینان حاصل شده و سپس نسبت به استفاده از آنها اقدام شود.

نکات امنیتی برای کاربران بانکداری اینترنتی

اطمینان از مجاز بودن درگاه

از درج اطلاعات مالی و بانکی خود از قبیل شماره حساب، شماره کارت، رمز، کد اعتبارسنجی (CVV2) و تاریخ انقضاء کارت در سایتهای متفرقه و مشکوک جدا خودداری و قبل از هر اقدامی از صحت مجاز بودن سایت مورد مراجعه اطمینان حاصل شود. امکان مشاهده و کنترل آدرس درگاهی مجاز بانک‌ها از طریق مراجعه به وب سایت رسمی بانک مرکزی ج.ا.ا (www.cbi.ir) وجود دارد. از معتبر بودن فروشگاه‌های خرید اینترنتی اطمینان حاصل شود. بسیاری از سوءاستفاده‌ها از طریق سایت جعلی، درج آرم بانک‌ها، بنرهای تبلیغاتی با محتوای امنیتی در سایت‌های مزبور و اخذ اطلاعات محرمانه کارت انجام می‌شود. هیچ سایتی به جز درگاه اینترنتی بانک‌ها مجاز به دریافت اطلاعات محرمانه کارت نیست.

خودداری از ذخیره اطلاعات در رایانه

هنگام استفاده از خدمات اینترنتی بانک‌ها و مؤسسات مالی یا خریدهای اینترنتی، از ذخیره‌کردن نام کاربری و رمز عبور در رایانه خودداری نمایید.

نکات امنیتی برای کاربران بانکداری اینترنتی

عدم نصب Key Logger

از عدم نصب Key logger های سخت‌افزاری و نرم‌افزاری بر روی رایانه‌ای که ثبت اطلاعات حساب بانکی از طریق آن صورت می‌گیرد، اطمینان حاصل شود.

اجتناب از ارایه مشخصات از طریق ایمیل و پیامک

از پاسخگویی به ایمیل و پیامکی که حتی به ظاهر از سوی بانک ارسال شده و از شما مشخصات و جزئیات کارت بانکی را درخواست می‌نماید جدا اجتناب شود. بسیاری از ارائه‌دهندگان خدمات پست‌الکترونیکی دارای گزینه‌ای برای اعلام ایمیل‌های مشکوک هستند (نظیر Report Spam). در صورت دریافت ایمیلی با چنین مضمونی توصیه می‌شود از گزینه مزبور جهت مسدود نمودن فرستنده استفاده شود.

اجتناب از نصب نرم‌افزار همراه‌بانک از طریق ایمیل

از نصب نرم‌افزارهای همراه‌بانک و مرتبط با کارت‌های بانکی که از طریق ایمیل دریافت می‌شود اجتناب و در صورت نیاز از طریق وب‌سایت اصلی بانک اقدام شود.

عدم استفاده از کامپیوترهای عمومی و شبکه

قویا توصیه می‌شود از مکان‌های عمومی ارائه دهنده خدمات اینترنتی مثل کافی‌نت‌ها، مراکز اینترنت، دانشگاه‌ها و سایر محل‌های نامطمئن، برای استفاده از خدمات بانکی اینترنتی استفاده نشود. ممکن است در رایانه‌های این گونه مراکز سخت‌افزار و نرم‌افزارهای خاصی برای سرقت نام کاربری و رمز عبور نصب شده باشد.

عدم استفاده از کامپیوترهای عمومی و شبکه

هنگام استفاده از اتصالات بی‌سیم (Wireless) امکان خطر شنود اطلاعات افزایش می‌یابد. تنها زمانی از اتصالات بی‌سیم استفاده شود که کاملا از امنیت ارتباط اینترنتی حصول اطمینان شده باشد.

استفاده از رمز یکبار مصرف

حتی‌الامکان از توکن و رمز عبور یکبار مصرف (OTP) جهت اتصال به درگاه اینترنتی بانک‌ها استفاده شود.

عدم تنظیم تلفن همراه در حالت خودکار

در استفاده از خدمات پرداخت سیار و بانکداری همراه می‌بایست تنظیمات تلفن همراه یا هر دستگاه قابل حمل دیگری در حالتی قرار گیرد که هنگام روشن شدن، کاربر ملزم به وارد نمودن رمز عبور بوده و از تنظیم نمودن آنها در حالتی که به‌صورت خودکار با حساب بانکی ارتباط برقرار کند، جدا خودداری شود. در صورت مفقود شدن یا به سرقت رفتن تلفن همراهی که به منظور پرداخت سیار و بانکداری همراه از آن استفاده می‌نمایید، لازم است مراتب در اسرع وقت به شرکت ارایه‌دهنده خدمات تلفن همراه و بانک اطلاع داده شود.

تغییر رمز عبور

رمز عبور خود را هر چند وقت یکبار تغییر دهید. حتما رمز «اینترنت‌بانک» حساب خود را به طول حداقل ۸ کاراکتر انتخاب کنید و آن را ترکیبی از حروف بزرگ و کوچک، اعداد و کاراکترهای ویژه نظیر« @ ، % » و ... باشد. ترکیب در هم ریخته‌ای از سال تولد و شماره‌شناسنامه و شماره‌ملی و ایمیل شما می‌تواند رمز خوبی برای «اینترنت‌بانک» شما باشد که به خاطرسپاری آن، سخت نخواهد بود.

استفاده از کامپیوترهای عمومی و شبکه

وسیله‌ای که (دسک‌تاپ، لپ‌تاپ، مینی‌لپ‌تاپ، تبلت، تلفن هوشمند و ...) با آن می‌خواهید وارد حساب «اینترنت‌بانک» خود شوید یا خرید اینترنتی انجام دهید، باید متعلق به خودتان باشد و عمومی نباشد. یعنی هرگز نباید از کافی‌نت و وسیله‌ای که متعلق به شما نیست، به «اینترنت‌بانک» حساب خود وارد شوید.

استفاده از آنتی ویروس به روز

اگر از کامپیوتر شخصی با سیستم‌عامل ویندوز استفاده می‌کنید (دسک‌تاپ، لپ‌تاپ، مینی‌لپ‌تاپ، تبلت) باید روی آن یک آنتی ویروس، یا بهتر است بسته امنیتی اینترنت (Internet Security) نصب شده باشد. اگر از تلفن‌های هوشمند و یا تبلت‌هایی با سیستم‌عامل غیر ویندوز استفاده می‌کنید (نظیر iOS و Android) بهتر است روی آن یک آنتی‌ویروس نصب کنید و سپس به حساب «اینترنت‌بانک» خود وارد شوید. اطمینان حاصل کنید، کامپیوتر شخصی که می‌خواهید از آن به حساب «اینترنت‌بانک» خود وارد شوید، فاقد بدافزار باشد.

اطمینان از به روز بودن مرورگر

هنگام ورود به حساب «اینترنت‌بانک» حتما از مرورگرهای به روز شده مطمئن استفاده کنید. حتی‌المقدور از مرورگرهایی که از طریق URL به درگاه پرداخت متصل می‌شوند مانند (Fire Fox) استفاده شود.

اجتناب از فیلتر شکن

هنگام اتصال به اینترنت برای استفاده از «اینترنت‌بانک» هرگز از وی.پی.ان، پروکسی و هرگونه فیلتر شکن استفاده نکنید.

نکات امنیتی برای کاربران بانکداری اینترنتی

چک کردن آدرس اینترنتی

حتما آدرس اینترنتی (URL) «اینترنت بانک» بانک مقصد را با دقت بررسی کنید که با https شروع شود، و از همان ترکیب و ترتیب حروف الفبایی باشد، که سایر صفحات وب سایت بانک مقصد از آن تشکیل شده‌اند. همیشه برای ورود به وبگاه بانک، نشانی آن را مستقیما در نوار نشانی مرورگر وارد کنید و از کلیک کردن روی لینک‌هایی که به مقصد وب‌گاه بانک به صورت ایمیل برای شما ارسال شده خودداری کنید. همچنین از لینک‌هایی که در ایمیل برای شما ارسال شده و به نظر می‌رسد از سوی بانک شما هم باشند به شدت بر حذر باشید؛ این حقه‌ای است که توسط خلافکاران به کار گرفته می‌شود تا شما را به وبگاهی درست شبیه بانک شما هدایت کند؛ وقتی به خیال خود وارد حساب بانکی خود شدید در واقع مشخصات ورود به آن را در اختیار دزدها قرار داده‌اید تا به سادگی حساب شما را خالی کنند.

استفاده از صفحه کلید مجازی

حتما هنگام وارد نمودن رمز عبور برای «اینترنت بانک» از صفحه کلید مجازی تعبیه شده در وب‌سایت بانک مقصد، یا صفحه کلید مجازی ویندوز استفاده کنید.

فعال کردن سیستم اطلاع رسانی پیامکی

حتما سرویس «اطلاع‌رسانی پیامکی» حساب خود را، همزمان با سرویس «اینترنت‌بانک» با هم فعال کنید، که هر زمان وارد اینترنت‌بانک خود شدید، از طریق یک پیامک به شما اطلاع داده شود.

خروج از اینترنت بانک پس از اتمام کار

حتما هنگام خروج از «اینترنت‌بانک» در وب‌سایت بانک مقصد، بر روی «خروج از اینترنت‌بانک» کلیک کنید و سپس مرورگر اینترنت را ببندید.

به طور دائم حساب خود را زیر نظر داشته باشید

حساب بانکی خود را حداقل به طور هفتگی بررسی کنید و از صحت تراکنش‌های طول هفته مطمئن شوید.