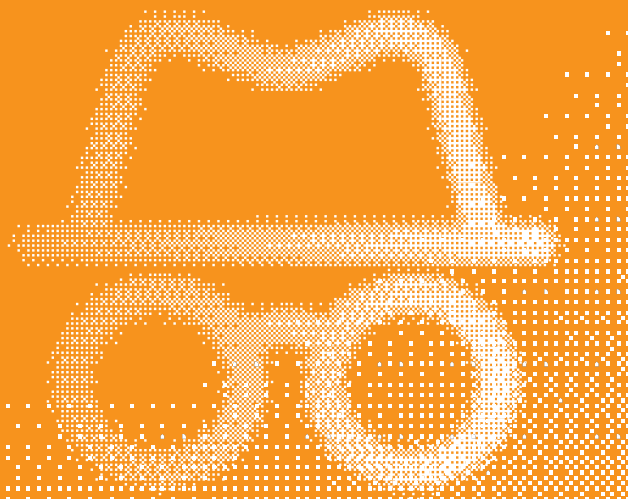
بانک خاورمیانه
Middle East Bank

پیشگیری از کلاهبرداری

نکات امنیتی برای دریافت خدمات حضوری و غیرحضوری



با پیشرفت فناوری، امروزه بانک‌ها خدمات خود را به‌صورت شبانه‌روزی، به مشتریان خود از طریق اینترنت‌بانک، موبایل‌بانک، دستگاه‌های خودپرداز و غیره ارائه می‌کنند.
در این شرایط، کلاهبرداران، غافل نبوده و تلاش می‌کنند با سرقت اطلاعات بانکی افراد، از حساب‌های آنها برداشت کنند.
در این بروشور، به نکاتی که امنیت کاربران اینترنتی و خدمات حضوری را تضمین می‌کنند، اشاره می‌کنیم.

نکات امنیتی برای خدمات غیرحضوری

نکات ابتدایی

- باز نکردن و بی‌توجهی به ایمیل‌های ناشناس
- پاسخ ندادن به ایمیل‌های درخواست‌کننده اطلاعات مالی یا شخصی شما
- پر نکردن فرم‌ها و صفحه‌های ورود متصل‌شده به این ایمیل‌ها
- ارسال نکردن رمز ورود از طریق ایمیل
- وارد نشدن به وب‌سایت‌های مشکوک

مراقبت از اطلاعات مالی

از انتشار اطلاعات مالی و بانکی خود از قبیل شماره‌حساب، شماره کارت، رمز، کد اعتبارسنجی (CVV۲) و تاریخ انقضای کارت در سایت‌های مشکوک (مانند خریدوفروش رمزارز و شرط‌بندی) و شبکه‌های اجتماعی و ذخیره کردن آنها در رایانه و موبایل خود، خودداری کنید. امکان مشاهده و کنترل آدرس درگاه مجاز بانک‌ها از طریق مراجعه به وب‌سایت رسمی بانک مرکزی ج.ا.ا. (cbi.ir) وجود دارد. از معتبر بودن فروشگاه‌های خرید اینترنتی نیز اطمینان حاصل کنید، چراکه بسیاری از سوءاستفاده‌ها از طریق سایت جعلی، درج نشان بانک‌ها، بنرهای تبلیغاتی با محتوای امنیتی و اخذ اطلاعات محرمانه کارت انجام می‌شود. به‌جز درگاه مجاز بانک‌ها، در هیچ وب‌سایت دیگری، اطلاعات بانکی خود را وارد نکنید.

بستن پنجره در زمان بروز خطا

در صورت بروز هرگونه اختلال حین فرآیند پرداخت اینترنتی که منجر به نمایش صفحه خطا روی مرورگر شود، صفحه را ببندید و عملیات پرداخت را از ابتدا انجام دهید.

عدم‌نصب Keylogger

از عدم‌نصب Keylogger سخت‌افزاری یا نرم‌افزاری بر روی رایانه‌ای که تراکنش بانکی از طریق آن صورت می‌گیرد، اطمینان حاصل کنید؛ به این منظور از رایانه‌های عمومی یا ناشناس استفاده نکنید و فقط نرم‌افزارهای موردنیاز را از منابع معتبر نصب کنید. هرگونه کندی غیرعادی یا رفتار مشکوک سیستم را به‌صورت جدی پیگیری کنید.

اجتناب از ارائه مشخصات از طریق ایمیل و پیامک

- از پاسخ به ایمیل و پیامک‌هایی که اطلاعات کارت بانکی شما را درخواست می‌کنند، پرهیز کنید.

بسیاری از ارائه‌دهندگان خدمات الکترونیکی، گزینه‌ای مانند "Report Spam" برای گزارش موارد مشکوک دارند. در صورت دریافت ایمیل با چنین مضمونی، از گزینه مزبور برای مسدود کردن فرستنده استفاده کنید.

نصب برنامک موبایل‌بانک از منابع مطمئن

- از نصب برنامک موبایل‌بانک و سایر برنامک‌های مرتبط با کارت‌های بانکی که از طریق ایمیل به شما ارسال شده‌اند، اجتناب کنید.
- برای دانلود برنامک موبایل‌بانک iOS فقط از استورهای معرفی‌شده در منوی موبایل‌بانک وب‌سایت بانک خاورمیانه استفاده کنید.
- برنامک موبایل‌بانک Android را می‌توانید به‌صورت مستقیم از وب‌سایت بانک خاورمیانه دریافت کنید.

عدم‌استفاده از کامپیوترهای عمومی و شبکه

- از مکان‌های عمومی ارائه‌دهنده خدمات اینترنتی مثل کافی‌نت‌ها، مراکز اینترنت، دانشگاه‌ها و سایر محل‌های نامطمئن، برای استفاده از خدمات بانکی اینترنتی استفاده نکنید. ممکن است در رایانه‌های این مراکز سخت‌افزار و نرم‌افزارهای خاصی برای سرقت نام کاربری و رمزعبور نصب شده باشد.

دقت در استفاده از اتصالات بی‌سیم

- هنگام استفاده از اتصالات بی‌سیم (Wireless) امکان خطر شنود اطلاعات افزایش می‌یابد؛ بنابراین فقط زمانی از اتصالات بی‌سیم استفاده کنید که کاملا از امنیت ارتباط اینترنتی اطمینان داشته باشید. فقط به شبکه‌هایی متصل شوید که رمزعبور قوی دارند و نام آنها را می‌شناسید و از اتصال به شبکه‌های عمومی فاقد رمز یا ناشناس خودداری کنید.

استفاده از رمز یک‌بارمصرف

- از رمزعبور یک‌بارمصرف (OTP) جهت اتصال به درگاه اینترنتی بانک‌ها استفاده کنید.

عدم‌تنظیم تلفن همراه در حالت خودکار

- در استفاده از خدمات بانکداری همراه باید تنظیمات تلفن همراه یا هر دستگاه قابل‌حمل دیگر را در حالتی قرار دهید که هنگام روشن شدن، ملزم به وارد کردن رمزعبور باشید. از تنظیم کردن آنها در حالتی که به‌صورت خودکار با حساب بانکی ارتباط برقرار کند، خودداری کنید. در صورت مفقود یا سرقت شدن تلفن همراه، در اسرع وقت به بانک اطلاع دهید.

فعال کردن سیستم اطلاع‌رسانی پیامکی

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

استفاده از آنتی‌ویروس به‌روز

- اگر از رایانه شخصی یا سیستم‌عامل ویندوز استفاده می‌کنید، باید روی آن یک آنتی‌ویروس به‌روزرسانی‌شده یا بسته امنیتی اینترنت (Internet Security) نصب شده باشد.
- اگر از تلفن‌های هوشمند یا تبلت‌هایی با سیستم‌عامل غیرویندوز استفاده می‌کنید (مانند iOS و Android) بهتر است روی آن یک آنتی‌ویروس نصب کنید و سپس به حساب اینترنت‌بانک خود وارد شوید. اطمینان حاصل کنید رایانه شخصی شما فاقد بدافزار یا ویروس باشد.

خروج از سامانه‌های الکترونیکی

- پس از اتمام کار در اینترنت‌بانک، از خارج شدن از سامانه اطمینان حاصل‌کنید.

اجتناب از نرم‌افزارهای مشکوک

- هنگام اتصال به اینترنت برای استفاده از اینترنت‌بانک، هرگز از VPN، پروکسی و فیلترشکن استفاده نکنید.

چک کردن آدرس اینترنتی

- اطمینان حاصل کنید که آدرس اینترنتی (URL) اینترنت‌بانک با https شروع شده و از همان ترکیب و ترتیب حروف الفبایی باشد که سایر صفحات وب‌سایت بانک از آن تشکیل شده‌اند.
- برای ورود به وب‌سایت بانک، نشانی آن را مستقیما در نوار نشانی مرورگر وارد کنید.
- لینک‌هایی که در ایمیل برای شما ارسال شده را هرگز باز نکنید؛ این حقه‌ای است که توسط کلاهبرداران به کار گرفته می‌شود تا شما را به وب‌سایتی درست شبیه بانک هدایت کنند. هنگامی که تصور می‌کنید وارد حساب بانکی خود شده‌اید، مشخصات ورود به آن را در اختیار سارقان قرار داده‌اید تا حساب شما را خالی کنند.

استفاده از صفحه‌کلید مجازی

- هنگام ورود اطلاعات از صفحه‌کلید مجازی تعبیه‌شده در وب‌سایت بانک موردنظر استفاده کنید.

کنترل دائم حساب‌های بانکی

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

نکات امنیتی برای خدمات حضوری

دقت در انتخاب رمزعبور

- رمزعبور ابزارها و سامانه‌های بانکداری الکترونیکی خود را هر سه ماه یک بار تغییر دهید.
- رمز اینترنت‌بانک حساب خود را به‌طول حداقل هشت کاراکتر (ترجیحا بیش از دوازده کاراکتر) انتخاب کنید که ترکیبی از حروف بزرگ و کوچک، اعداد و کاراکترهایی مانند @، ٪ و غیره باشد.
- از رمزعبورهای قابل‌حدس مانند سال تولد، شماره شناسنامه و غیره استفاده نکنید.
- از یادداشت رمزعبور سامانه بانکداری اینترنتی خود و استفاده رمزهای یکسان برای کارت‌ها و سامانه‌های بانکی خودداری کنید.
- رمزعبور ابزارها و سامانه‌های بانکداری الکترونیکی خود را در اختیار دیگران، قرار ندهید.

اطمینان از به‌روز بودن مرورگر

- هنگام ورود به اینترنت‌بانک حتما از مرورگرهای به‌روزرسانی‌شده قابل‌اعتماد (مانند Microsoft Edge، Safari، Google Chrome و Firefox) استفاده کنید.

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 دستگاه‌های خودپرداز و پایانه‌های فروشگاهی را در محل رها نکنید.

حفظ امنیت در وارد کردن رمز

- در مکان‌های عمومی برای محافظت از اطلاعات محرمانه، هنگام استفاده از کارت و وارد کردن رمزعبور در دستگاه‌های خودپرداز یا پایانه‌های فروشگاهی، با استفاده از دست دیگر خود یک سپر حفاظتی ایجاد کنید.

توجه به وضعیت خودپرداز

- در صورت مشاهده وضعیت غیرعادی روی دریچه ورودی کارت یا خروجی وجه دستگاه‌های خودپرداز (مانند چسب‌خوردگی و وجود شی اضافه)، ضمن اعلام مراتب به مسئولان شعبه در ساعات کاری و مرکز ارتباط مشتریان بانک (آشنا) در سایر ساعات شبانه‌روز، از دستگاه خودپرداز دیگری استفاده کنید.

خودداری از ارائه رمز کارت به فروشنده

- از ارائه رمزعبور به فروشنده‌ها خودداری کرده و شخصا رمز خود را در پایانه‌های فروشگاهی وارد کنید.

رعایت فاصله در زمان استفاده از خودپرداز

- در زمان استفاده از دستگاه‌های خودپرداز دقت کنید که فاصله مناسب نفر بعدی با شما رعایت شده باشد. رعایت این نکته نشانه حفظ حریم خصوصی و به‌تبع آن افزایش امنیت استفاده‌کننده از دستگاه‌های خودپرداز است.

کنترل وجه دریافتی

- پس از دریافت کارت و وجه از دستگاه‌های خودپرداز، در مکانی امن وجه دریافتی را شمارش کنید.

مسدود کردن کارت مفقودشده

- به‌محض اطلاع از مفقود شدن کارت بانکی خود، آن را مسدود کنید. روش‌های مسدود کردن کارت عبارتند از: اینترنت‌بانک، موبایل‌بانک، دستگاه‌های خودپرداز، مراجعه به شعب بانک و تماس با مرکز ارتباط مشتریان بانک (آشنا) .

تغییر دوره‌ای رمز کارت

- سالانه چندبار، رمز کارت‌های بانکی خود را تغییر دهید و از انتخاب رمزهای یکسان برای همه کارت‌های بانکی خودداری کنید.

سایر موارد امنیتی

- مطمئن شوید که اطلاعات تماس شما در سامانه بانکداری الکترونیکی صحیح است و در صورت تغییر آن را به‌روزرسانی کنید.

بانک خاورمیانه
Middle East Bank

ساختمان ادارات مرکزی

ساختمان شماره ۱
تهران، خیابان احمد قصیر (بخارست)
نبش خیابان پنجم، شماره ۲
تلفن ۸۰۰۰ ۴۲۱۷ (۰۲۱)
دورنگار ۲۳۸۳ ۹۱۲۱ (۰۲۱)
کدپستی ۱۵۱۳۶۴۵۷۱۷

ساختمان شماره ۲
تهران، خیابان احمد قصیر (بخارست)
خیابان ششم، شماره ۲۶
تلفن ۹۰۸۱ ۸۸۵۰ (۰۲۱)
دورنگار ۶۹۴۹ ۸۸۷۵ (۰۲۱)
کدپستی ۱۵۱۴۶۴۴۱۱۴

صندوق پستی ۴۴۴۵-۱۵۸۷۵
www.middleeastbank.ir
info@middleeastbank.ir

آشنا (مرکز ارتباط مشتریان) ۵۵۷ ۴۲ (۰۲۱)
رسیدگی به شکایات (مدیریت بازرسی) ۸۸۸۸ ۴۲۱۷ (۰۲۱)

برای کسب اطلاعات بیشتر درباره پیشگیری از کلاهبرداری QRکد را اسکن کنید.

مهر ۱۴۰۴