توصیه‌های امنیتی سامانه معاملات برخط

مدیریت کلمه عبور

- **لطفاً شناسه مشتری و کلمه عبور سامانه معاملات برخط ارائه شده توسط کارگزاری را در اولین ورود به سامانه مذکور تغییر دهید.**

- توصیه می‌گردد کلمه عبور سامانه معاملات برخط ، ترکیبی از حروف بزرگ و کوچک، اعداد و کاراکترهای ویژه نظیر @،٪، $ و غیره باشد.

- کلمه عبور سامانه معاملات برخط خود را در اختیار دیگران قرار نداده و آن را در فواصل زمانی (حداقل هر سه ماه) و بنا به ضرورت تغییر دهید.

- از انتخاب کلمه عبور قابل حدس نظیر سال تولد، سال ازدواج، شماره شناسنامه و ...، برای ورود به سامانه معاملات برخط خود، اجتناب نمایید.

- هنگام ورود شناسه مشتری و کلمه عبور سامانه معاملات برخط ، از عدم رویت آن توسط دیگران اطمینان حاصل نمایید.

- از یادداشت و ذخیره نمودن شناسه مشتری و کلمه عبور سامانه معاملات برخط در جایی که امکان سوءاستفاده‌های آتی از حساب بانکی شما را برای یابنده آن فراهم می‌نماید، خودداری نمایید.

- از انتخاب رمزهای مشابه برای کارت‌ها و سامانه‌های بانکی خودداری نمایید.

پیشگیری از سوءاستفاده‌های اینترنتی

- سوءاستفاده‌های اینترنتی به منظور دسترسی به اطلاعات محرمانه بانکی به روش‌های گوناگونی توسط کلاهبرداران انجام می‌گردد. در یکی از این روش‌ها (فیشینگ) کلاهبرداران از طرق مختلف نظیر ایجاد وب‌سایت‌های جعلی مشابه با وب‌سایت‌های اصلی و معتبر، ارسال ایمیل و پیامک به منظور سرقت اطلاعات محرمانه و سوءاستفاده از این اطلاعات اقدام می‌نمایند. به منظور جلوگیری از قرارگرفتن در معرض جعل و سوءاستفاده اینترنتی توصیه

می‌شود برای امنیت بیشتر، وب‌سایت کارگزاری ستاره جنوب را با تایپ نمودن نشانی اینترنتی (URL) آن در نوار آدرس(Address bar) مرورگر وب مشاهده نمایید.

- از باز کردن ایمیل‌های ناشناس و پاسخ به نامه‌ای که در آن درخواست اطلاعات شخصی، مشخصات و جزئیات حساب بانکی، کارت بانکی و ... را می‌نماید، اجتناب کنید.
- از ورود به وب‌سایت‌های متفرقه و بازنمودن لینک‌های مربوطه اجتناب نمایید.
- ملاحظات رایانه، تبلت و گوشی تلفن همراه هوشمند:
- همواره از عدم نصب ابزارهای سرقت کلمه(key logger) سخت‌افزاری و نرم‌افزاری بر روی رایانه خود اطمینان حاصل نمایید.
- از دریافت(Download) و اجرای نرم‌افزار و فایل‌های ناشناس و متفرقه روی رایانه، تبلت و گوشی تلفن همراه خود اجتناب نمایید.
- از بروزرسانی مستمر سیستم عامل، مرورگر وب و سایر نرم‌افزارهای منصوب روی رایانه، تبلت و گوشی تلفن همراه خود اطمینان حاصل نمایید.
- رایانه، تبلت و گوشی تلفن همراه خود را به ضد ویروس معتبر مجهز نموده و آن را به صورت مستمر بروزرسانی نمایید.
- برای دسترسی به سامانه معاملات برخط از ابزارهای فیلتر شکن نظیرVPN استفاده ننمایید.
- پس از اتمام کار در سامانه بانکداری اینترنتی، با استفاده از گزینه خروج، از سامانه مذکور خارج شوید.
- رایانه، تبلت و گوشی تلفن همراه خود را طوری تنظیم نمایید که در فواصل زمانی کوتاه با استفاده از روش‌های امنیتی(PIN,Pattern, Password و ...) قفل گردد.

ملاحظات عمومی

- از صحت اطلاعات در سامانه معاملات برخط اطمینان حاصل نموده و در صورت تغییر اطلاعات مزبور نسبت به بروزرسانی آن‌ها از طریق مراجعه به کارگزاری ، اقدام نمایید.

- تا حد امکان از محیط‌های عمومی (نظیر کافی‌نت) رایانه‌های ناشناس و شبکه‌های بی‌سیم عمومی برای دسترسی به سامانه معاملات برخط اجتناب نموده و در صورت استفاده حتماً در اولین فرصت ممکن کلمه عبور خود را تغییر دهید.

- هرگز اطلاعات مهم خود مانند رمز اول و دوم کارت‌ها، کلمه عبور سامانه‌های بانکی،CVV۲، تاریخ انقضای کارت را بر روی گوشی تلفن همراه ذخیره ننموده یا از طریق پیامک، ایمیل و سایر سامانه‌های ارتباطی نظیر تلفن برای سایرین ارسال و بازگو نکنید.

- کارگزاری هرگز اطلاعات محرمانه شما (نظیر مشخصات شناسنامه‌ای، کدملی، اطلاعات مربوط به کارت و حساب بانکی و ...) را از طریق تلفن، ایمیل یا پیامکدرخواست نمی‌کند. در صورت رخداد این مورد، ضمن عدم پاسخگویی به چنین درخواست‌هایی مراتب را سریعاً به کارگزاری اطلاع دهید.

- هرگز اطلاعات مربوط به حساب و کارت بانکی خود را در شبکه‌های اجتماعی قرار ندهید.

- سایت پلیس فتا به آدرس www.cyberpolice.ir مرجع مفیدی برای دریافت آخرین اطلاعات مربوط به تهدیدات امنیتی است.