Сигурносни препораки за електронска комуникација со Силк Роуд Банка АД Скопје

Почитувани клиенти,

Следејќи ја определбата на Банката, клиентите во центарот на вниманието, СилкРоуд Банка Ви укажува на одредени сигурносни аспекти и препораки кои треба да ги применувате при користење на електронските услуги на Банката. Банката обезбедува три вида на електронска комуникација со своите клиенти и тоа:

- Преку веб страната за електронско банкартство https://silkroad.24x7.com.mk/Retail/Account/Login
- Преку веб страната за сигурна достава на електронска пошта https://keys.silkroadbank.com.mk
- Преку мобилната апликација за Андроид и IOS Silk Road m-Bank

За воспоставување на ефикасна безбедносна заштита, покрај мерките преземени од страна на Банката, потребна е едукација и соработка со вас, почитувани клиенти.

Лозинки

Прв чекор за заштита од злоупотреба е креирање на сложена лозинка.

Лозинката не треба да содржи ваши лични податоци, семејни имиња, значајни датуми и податоци што лесно можат да се погодат. Исто така, не треба да се користат генерички зборови и последователни секвенци (P@ssword, Admin, 1234567890, Administrator, user и сл.)

Со цел полесно да ги помните лозинките може да дефинирате Ваше лично правило според кое ќе ги креирате идните лозинки.

Не го запишувајте Вашето корисничко име и лозинка на хартија што ја носите со себе или во Вашиот мобилен телефон. Доколку имате потреба, запишете ги и чувајте ги на сигурно место кое само Вие го знаете. Пожелно е корисничкото име и лозинката да ги чувате на различно место, за да оневозможите неовластен пристап при евентуално губање или кражба.

Не го користете истото корисничко име и лозинка за пристап до други web страници, бидејќи ако лозинката се дознае на било кој од тие страници, ќе може да се употреби и за електронското банкарство.

Менувајте ја лозинката на одреден период (на пример 3 месеци) за да го намалите ризикот од злоупотреба при евентуална нејзина кражба.

Лозинката не ја споделувајте со никого. Ако на некој од вашето семејство или на вашите вработени им е потребен пристап до сервисите, регистрирајте посебна корисничка сметка со посебно корисничко име и лозинка за пристап.

Доколку ја заборавите Вашата лозинка, во случај кога се работи за електронското банкарство, преку следниот линк: https://secure.24x7.com.mk/enrollment_silkroad/mk-MK/Retail/ResetAccount (заборавена лозинка или корисничко име), можете да креирате

нова лозинка. За промена на нова лозинка на електронско банкарство потребно е да поседувате дебитна картичка во Банката. Доколку имате било каков проблем јавете се на телефонскиот број за техничка поддршка +389 2 3289-440.

Доколку ја заборавите Вашата лозинка во случај кога се работи за пристап кон системот за сигурна достава на електронска пошта, тогаш користете ја опцијата за заборавена лозинка (I lost my passphrase), а доколку имате проблеми јавете се на бројот +389 2 3289 430.

Користење на јавни мрежи и компјутери

Избегнувајте го користењето на сервисите за електронско банкарство преку отворен безжичен интернет пристап (аеродроми, ресторани, трговски центри...) освен ако интернет пристапот не е соодветно заштитен (WPA, WPA2 , VPN или 4G).

Не пристапувајте до сервисите за електронско банкарство од јавен компјутер. Секогаш користете свој компјутер. Доколку сепак сте се најавиле на електронсото банкарство од потенцијално компромитиран компјутер, при првата можност од Вашиот компјутер сменете ја Вашата лозинка.

Пристап до електронско банкарство и системот за сигурна достава на мејл пораки од проверен линк

- Секогаш пристапувајте до сервисите за електронско банкарство така што во интернет пребарувачот ќе ја внесете адресата: https://silkroad.24x7.com.mk/Retail/Account/Login .

Никогаш не користете линкови добиени по мејл или изложени на трети страни за да пристапите на страната за електронско банкарство. Најчестиот напад што може да се случи е т.н. phishing напад, во кој напаѓачот Ви праќа линк до лажна WEB страна, која е идентична со оригиналната за Вие да го оставите своето корисничко име и лозинка и да станете жртва за понатамошна злоупотреба. Секогаш проверувајте ја валидноста на линкот и сертификатот во линијата за адреса на вашиот пребарувач.

Дококу Банката има потреба да Ви испрати мејл со доверлива содржина, тоа ќе биде направено преку системот за сигурна достава на мејл пораки PGP Web Messenger. Всушност се работи за посебен WEB портал во сопственост на нашата Банка.

Пристапувајте до сервисот за сигурна достава на мејл пораки користејки го линкот добиен на Вашата мејл адреса и притоа секогаш проверете дека испраќачот е paymentoperations@silkroadbank.com.mk. Исто така проверете дека во субјектот на пораката се наоѓа бројот на вашата сметка. Линкот во пораката секогаш треба да почнува со: https://keys.silkroadbank.com.mk, а во него е содржан и називот на вашата мејл адреса.

Одјавување од електронското банкарство и системот за сигурна достава на мејл пораки

По завршување на потребата од користење на сервисите за електронско банкарство и системот за сигурна достава на мејл пораки, секогаш одјавете се и проверете дали сте успешно одјавени. Секое оставање на отворена сесија откако сте го напуштиле компјутерот, отвара можност потенцијален напаѓач кој се нашол во физичка близина да изврши злоупотреба на Вашите банкарски сметки, иако не ја знае Вашата лозинка, или да дојде до доверлива содржина што Вас Ви била испратена.

Не споделувајте податоци

Банката никогаш нема да Ве праша за Вашата лозинка за најава на сервисите за електронско банкарство. Доколку добиете e-mail порака во која се бара Вашата лозинка и/или корисничко име, или порака во која се бара да ја "потврдите" или да ја "ажурирате" корисничката лозинка, тоа е обид за кражба на Вашата лозинка/корисничко име. Не кликајте на линковите во e-mail пораката, а пораката избришете ја веднаш.

Банката никогаш нема да Ви побара да внесете број на платежна картичка, ПИН, сигурносен трицифрен код на позадината на картичката (за авторизација на трансакции преку интернет) или други лични податоци бидејќи користењето на сервисите за електронско банкарство не зависи од бројот на вашата платежна картичка или ПИН. За користење на сервисот за електронско банкарство во строго контролирана постапка Вам Ви е доделен активациски код на смс порака со помош на кој Вие го активирате Вашиот кориснички профил и потоа креирате Ваша лозинка,која ја знаете само Вие.

Никогаш не ги давајте Вашите лични податоци или финансиски информации на непознати лица кои Ве контактираат од компании со кои никогаш претходно не сте комуницирале, а Ве контактираат по пат на e-mail, телефон или писмено. Истото важи и за агенции кои се претставуваат како консултанти, извршители или маркетинг агенции на компанија со која веќе имате воспоставено деловен однос. Банката никогаш нема да Ве контактира на ваков начин, бидејќи согласно Законот за заштита на лични податоци и интерните акти на Банката без ваша писмена согласност ниту една ваша контакт информација како што е тел. број, e-mail адреса или домашна адреса не смее да биде дадена на трета страна.

Следење на сметките и трансакциите

Редовно проверувајте ги вашите трансакции и доколку забележите трансакција за која не сте сигурни дека сте ја авторизирале или не соодветствува на набавените производи и услуги, макар и да е мала сума, веднаш јавете се на телефонскиот број: +389 2 3289 440 и побарајте понатамошни инструкции.

Ако сте изгубиле ливче на кое сте го запишале Вашето корисничко име или лозинка, обидете се да се најавите на сервисите за електронско банкарство и веднаш сменете ја корисничката лозинка. Доколку не можете да се најавите, случајот пријавете го на телефонскиот број: +389 2 3289 440 и побарајте блокирање на пристапот до електронското банкарство од вашето корисничко име и креирајте нова лозинка.

Надградби на ОС, антувирус и заштитни програми

На Вашиот компјутер користете ажуриран антивирус софтвер, поставете огнен ѕид и заштитни програми. Пожелно е да користите квалитетен антивирус, кој покрај од вируси нуди заштита од други типови злонамерни програми (spyware, тројанци), детектира малициозни активности на компјутерот, предупредува и блокира посета на малициозни или заразени web-страни итн. Изберете софтвер препорачан од повеќе доверливи и независни извори.

Следете ги предупредувањата за вируси, а особено за тројанци од Вашиот антивирус софтвер. Овие злонамерни програми обично се инсталираат автоматски, со кликање на линк или отварање на апликации кои сте ги добиле прикачени во e-mail порака или при инсталирање на пиратски софтвер.

Секогаш користете последна верзија од Вашиот интернет пребарувач со сите безбедносни ажурирања.

Редовно ажурирајте го софтверот на Вашиот компјутер. Не користете застарени оперативни системи за кои производителот престанал да издава сигурносни надградби. На овој начин ќе обезбедите Вашиот оперативен систем, антивирусните и останатите заштитни програми да Ви овозможат најдобра заштита.

За работа на Вашиот компјутер, а особено при користење на интернет, работете со корисник кој нема администраторски привилегии.

Идентификација на web страната

Интернет страната за електронско банкарство на СилкРоуд Банка може да се идентификува преку соодветен серверски сертификат издаден од страна на DigiCert издаден на silkroad.24x7.com.mk.

На страната https://silkroad.24x7.com.mk/Retail/Account/Login , до полето за адресата или во долниот дел на пребарувачот (зависно од пребарувачот што го користите) се појавува катанче на кое може да се видат овие информации.

Сомневање за кражба или злоупотреба

Доколку не се придржувате до овие препораки, може да се случи т.н. кражба на идентитетот при што потенцијалниот напаѓач кој ќе дојде до вашите податоци за идентификација, може лажно да се претстави како Вас, со што ќе му биде дозволен пристап до Вашите сметки и вршење трансакции без знаење на Банката.

Во случај на сомнеж од кражба или злоупотреба:

- Веднаш сменете ја лозинката за пристап користејќи доверлив компјутер;
- Може да го блокирате Вашиот кориснички профил со јавување на телефонскиот број +389 2 3289 440. По блокирањето, ниту Вие, ниту потенциланиот напаѓач, нема да може да се најави во сервисите за електронско банкарство за увид или вршење трансакции;
- Проверете го датумот на последна активност во електронското банкарство.

Секој обид за доаѓање до ваши податоци од страна на било кое лице, лично, по телефон или преку интернет, сметајте го за обид за кражба и пријавете го на +389 2 3289 440. Дополнително, имате право случајот да го пријавите и во МВР и во Дирекцијата за заштита на лични податоци.