

Банктің мобильді қосымшасында жұмыс істеу кезіндегі қауіпсіздік жөніндегі Жадынама

Банк сервисі пайдаланушыларға жасалған банктік қызмет көрсету шарттары және/немесе электрондық ақша қаражаты шарты шеңберінде банкпен өзара іс-қимылды жүзеге асыруға мүмкіндік беретін банктің мобильді қосымшасы болып табылады, сондай-ақ ақпарат алмасуды және Интернет арқылы немесе мобильді құрылғының (смартфон, планшет және т. б.) арнайы қосымшасы арқылы жекелеген операцияларды жасауды қоса, осындай қорытындысыз, сондай-ақ мобильді құрылғыларды пайдаланушыларға қызметтерге ақы төлеуге, жеке тұлғалар арасында банк сервистері арқылы ақша аударымдарын жүзеге асыруға және Интернетте сатып алулар жасауға мүмкіндік беретін электрондық төлемдер жүйесі.

Қауіпсіздіктің негізгі ережелерімен танысыңыз:

- ✓ Интернет желісінде және банк сервистерін пайдалану кезінде пайдаланылатын SMS-хабарламадан бір реттік парольді ешкімге бермеңіз және айтпаңыз;
- ✓ банк қызметтерін қосу кезінде үшінші тұлғалардың ұялы телефон номерлерін пайдаланбаңыз;
- ✓ төлем Карточкасының деректемелерін, сондай-ақ 3D Secure CVC/CVC2-код/пароль деректерін ешкімге хабарлауға немесе бермеңіз;
- ✓ ешқандай жағдайда SMS-хабарламадан кодты ұсыну талап етілетін кеңес немесе қызметті алу үшін Банктің Байланыс орталығына өз бетінше жүгінген жағдайларды қоспағанда, өз логиніңізді, пароліңізді, SMS-хабарламадан кодты ешкімге, оның ішінде банк қызметкерлеріне жария етпеңіз. Жеке құпия деректер мен парольдерді сақтау үшін жауапкершілік пайдаланушыға жүктеледі;
- ✓ бұл басқа біреудің мобильді құрылғысында саусақ ізі арқылы ПИН-кодты немесе кіруді орната отырып, Банктің мобильді қосымшаларында авторизацияны жүргізбеңіз;
- ✓ күн сайын банк қабылдаған және қабылдамаған операциялар туралы барлық хабарламаларды талдап отырыңыз, сондай-ақ ақшаны санкцияланбаған есепке алу (аудару) жағдайлары туралы Банкке дереу хабарлаңыз;
- ✓ ұялы телефон жоғалған/ұрланған жағдайда Банк растайтын бір реттік парольмен SMS-хабарламалар жібереді немесе SIM-Картаның жұмысы күтпеген жерден тоқтатылады, сіз ұялы байланыс операторына мүмкіндігінше тезірек хабарласып, SIM-Картаны бұғаттауыңыз керек, сондай-ақ бұл туралы Банкке дереу хабарлаңыз;
- ✓ «SMS-ақпараттандыру» қызметін қосыңыз, Интернет желісіндегі Карточкалық операцияларға лимиттер орнатыңыз;
- ✓ мобильді құрылғының операциялық жүйесін жаңартуларын уақытында орнатыңыз;
- ✓ лицензияланған антивирустық бағдарламалық жасақтаманы қолданыңыз және оны үнемі жаңартып отырыңыз;
- ✓ зиянды бағдарламаларды уақытында анықтау үшін антивирустық тексеруді үнемі жүргізіп отырыңыз;
- ✓ үшінші тұлғалардың немесе бейтаныс адамдарың сұрауы бойынша бөгде қосымшаларды орнатпаңыз;
- ✓ Банк барлық қажетті ақпаратқа ие және ешқашан, ешбір жағдайда төлем Карточкасының деректемелерін, авторизациялық деректерді, төлем Карточкасына ПИН-кодты беруді сұрай отырып, телефон арқылы электрондық хабарламаларды, SMS-хабарламаларды, қоңырауларды жіберуді жүзеге асырмайды, сондай-ақ бағдарламаларды және олардың жаңартуларын электрондық пошта арқылы таратпайды;
- ✓ деректер бұзылған немесе рұқсат етілмеген қол жеткізу фактілері анықталған және мобильді қосымша арқылы банктік шоттардан рұқсат етілмеген транзакциялар жүргізілген жағдайда Сізге дереу 595 номері бойынша Байланыс орталығына (ҚР

бойынша тегін қоңырау шалу) немесе security@.kz электрондық мекенжайына хабарласу қажет.