МОБИЛЬДІ ҚОСЫМШАНЫ/ТӨЛЕМ ҚОСЫМШАСЫН ПАЙДАЛАНУ КЕЗІНДЕГІ ҚАУІПСІЗДІК БОЙЫНША КЕҢЕСТЕР

- *Мобильді қосымшада/Төлем қосымшасында тек жеке мобильді құрылғы арқылы тіркеліңіз.*
- *Дебеттік/кредиттік карта нөмірлері, CVC/CVV2/CVP2 коды немесе ПИН-код сияқты құпия ақпаратты мобильді құрылғыда (смартфон/планшет және т.б.) сақтамаңыз.*
- *Белгісіз көздерден мобильді қосымшаларды жүктемеңіз. Қосымшалардың ресми дүкендерін пайдаланыңыз (Apple Store, Google Play, Банктің ресми сайты арқылы).*
- *Мобильді құрылғыға тиімді вирусқа қарсы бағдарламалық жасақтаманы орнатыңыз және оны үнемі жаңартып отырыңыз.*
- *Мобильді құрылғылардың операциялық жүйелерінің ресми жаңартуларын уақытылы орнатыңыз.*
- *Жаңа қосымшаны орнату кезінде рұқсаттарға назар аударыңыз. Егер рұқсаттар күдік тудырса немесе бағдарламаның функционалына сәйкес келмесе, оны пайдаланудан бас тартқан дұрыс.*
- *Банк Сізге бір реттік құпиясөзбен растайтын SMS-хабарламалар жіберетін мобильді құрылғыға кіру мүмкіндігін жоғалтқан кезде, ұялы телефонды бұғаттау үшін ұялы байланыс операторына, сондай-ақ Банктің Байланыс орталығына дереу хабарласу қажет.*
- *Сіз өзіңіздің карталық операцияларыңызға лимиттер қоя отырып және «SMS-хабарламалар»/ «Push-хабарландырулар» қызметін пайдалана отырып, қауіпсіздік деңгейін арттыра аласыз.*
- *Телефон нөмірін жоғалтқан/ауыстырған жағдайда бұл туралы міндетті түрде Байланыс орталығына (5030 немесе 8-8000-80-60-60) немесе Банк бөлімшесіне хабарлаңыз.*
- *Мобильді құрылғыны ауыстыру кезінде ескі құрылғыдан Банктің мобильді қосымшасын, сондай-ақ төлем қосымшаларында (Apple Pay/Samsung Pay/Google Pay/Mir Pay) тіркелген төлем карталарын міндетті түрде өшіріңіз.*
- *Rooting немесе jailbreak операцияларын орындау арқылы мобильді құрылғы өндірушісі орнатқан шектеулерді алып тастамаңыз. Бұл өндіруші енгізген қауіпсіздік функцияларының тиімділігін едәуір төмендетеді, нәтижесінде сіздің мобильді құрылғыңыз вирустық бағдарламалық жасақтаманы жұқтыруға осал болады.*
- *Операциялар орындалғаннан кейін Мобильді қосымшаның/Төлем қосымшасының жұмысын әрдайым аяқтаңыз (мобильді құрылғыны бұғаттау арқылы) немесе аккаунттардан шығыңыз.*
- *Мобильді құрылғыға кіру үшін құпиясөзбен қорғауды орнатыңыз, бұл мүмкіндік кез келген мобильді құрылғылар үшін қолжетімді.*
- *Құпиясөздердің қарапайым комбинацияларын пайдаланбаңыз, мысалы, 0000, 7777, 1234 және т.б.*
- *Қоғамдық сенімсіз Wi-Fi желілерін пайдаланбауға тырысыңыз (мысалы, кафелерде, сауда орталықтарында және т.б.).*
- *Мобильді құрылғыларға қашықтан кіру қосымшаларын орнатпаңыз (мысалы, anydesk, radmin және т.б.).*
- *Банктен алынған «SMS-хабарламаларды»/ «Push-хабарландыруларды» үшінші тұлғаларға ешқашан хабарламаңыз (Банк қызметкерлері мұндай деректерді сұрамайды).*