Қажетті қаупсіздік шараларына қатысты ұсыныстар

- Сізге банк берген карточканы пайдалану ережелерін оқыңыз. Егер қандай да бір ережелер Сізге түсініксіз болса, банктің қызметкерлерімен байланысыңыз.
- Банктен карточкаларды алған кезде олардың тиісті жерлеріне жеке қолтаңбаңыздың үлгісін міндетті түрде қойыңыз.
- Өз карточкаңызды ешқашан қараусыз қалдырмаңыз, оны қауіпсіз жерде сақтаңыз.
- Сатып алуды төлем карточкасымен төлей отырып, ол бойынша барлық операциялар Сіздің қатысуыңызбен жасалуына тырысыңыз. Сатушының/даяшының Сіздің карточкаңызды басқа жайға алып кетуіне рұқсат бермеңіз, операциялардың Сіздің қатысуыңызбен жүргізілуін талап етіңіз.
- Егер Сіз сатып алудан бас тартсаңыз немесе егер чекті немесе слипті ресімдеу кезінде қателік жіберілсе, бүлінген чектің/слиптің Сіздің қатысуыңызбен жойылуын сұраңыз, ал екінші данасын өзіңізбен бірге ала кетіңіз және бір ай бойы сақтаңыз (карточкалық есеп бойынша көшірмемен салыстыруға дейін).
- Мүмкіндігіне қарай өз карточкаңызды интернетте пайдаланбаңыз, Сіздің карточкаңыздың деректемелерін (карточка нөмірін, CVC2 – Card Verification Code 2 арнайы кодын, қолданыс мерзімін) электронды почта бойынша бермеңіз. Операцияларды интернет желісінде жүргізу үшін VISA VIRTUON карточкасын пайдалануды ұсынамыз, ол тауарлар мен қызметтерді төлеу кезінде алаяқтық транзакциялар тәуекелін біршама азайтады.
- Ешқашан ПИН-кодты (дербес сәйкестендіру нөмірін) карточкаға жазбаңыз. ПИН-кодты есте сақтау керек. Егер Сіз дегенмен де ПИН-кодты жазып қойсаңыз, мұны Сізден басқа ешкімге белгілі болмайтындай етіп шифрлы түрінде жасаған дұрыс және оны ешқашан карточкамен бірге алып жүрмеңіз.
- Өз ПИН-кодыңызды ешқашан жарияламаңыз, Сіз оны ешкімге: банктің қызметкерлеріне де, құқық қорғау органдарының өкілдеріне де, сауда орындарының кассирлеріне де хабарлауға міндетті емессіз. Тек карточканы ұстаушы ғана өз ПИН-кодын білуі тиіс.
- Карточканы жоғалтып немесе ұрлатып алған жағдайда, ол бойынша алаяқтықты болдырмау үшін банктің қызметкерлері карточканы оқшаулауды жүзеге асыруы үшін дереу банкке немесе Байланыс Орталығына жүгіну қажет.
- Өз карточкаңызды үшінші тұлғаларға: досыңызға, жұбайыңызға, әсіресе олар шетелге баратын болса, ешқашан бермеңіз. Егер банкомат қандай да бір себеп бойынша карточканы алып қойса, онда Сіз бен жақындарыңыз үшін проблема туындауы мүмкін.
- Сіздің отбасы мүшелерінің қосымша карточкаларды пайдалануын бақылаңыз. Сіз қосымша карточкалар арқылы жүргізілген барлық операциялар бойынша толықтай жауап бересіз.
- Шот бойынша үзінді көшірмені ұдайы тексеріп отырыңыз. Сіз күдікті операцияларды неғұрлым тезірек тапсаңыз және хабарлайтын болсаңыз, соғұрлым жақсы болады. Шағым жасау үшін қатаң белгіленген мерзімдер бар, оның барысында Сіз және банк шаралар қабылдай аласыздар. Чектерді сақтаңыз және оларды карточканың есебі бойынша үзінді көшірмемен салыстырыңыз. Өзіңіздің карточкалық шотыңыз бойынша қалдықты жиі тексеріп тұрыңыз.
- Сіз өз қалауыңыз бойынша шығыстардың апта сайынғы немесе ай сайынғы лимиттерін белгілеу үшін банкке жүгіне аласыз. Бұл Сіздің есебіңізді алаяқтықтан қосымша қауіпсіздендіреді.
- Банктен қандай да бір дербес деректерді беру деген мақсатпен хабарламаны алған жағдайда, өзіңізге белгілі телефон нөмірі бойынша дереу банкпен хабарласыңыз.
- Сіздің карточкаңыздың деректемелері бөтен тұлғаларға белгілі болды деп күдіктенетін болсаңыз, бұл жөнінде өз банкіңізге дереу хабарлаңыз.

1. БАНКОМАТ АРҚЫЛЫ ОПЕРАЦИЯЛАРДЫ ЖҮРГІЗУ КЕЗІНДЕГІ ҚАУІПСІЗДІК ШАРАЛАРЫ:

- Банкоматта қолма-қол қаражаттарды алған кезде Сіз өзіңізге керекті төлем жүйесінің карточкаларына қызмет көрсететініне көз жеткізуіңіз қажет (әдеттебанкоматтардабанкоматтың қандай төлем жүйелерінің карточкаларына қызмет көрсететіні туралы клиенттерді хабарландыратын жапсырмалар орналасады).
- Операцияларды банкомат арқылы жүргізудің алдында жағдайды бағалау қажет. Банкоматтың бұзылуының қандай да бір сыртқы белгілерін көріп, бұл жөнінде банкке хабарлаңыз және басқа банкоматты пайдаланыңыз.
- Экранында басқа банкоматтарға өту туралы өтініш хабарламасы көрсетілетін банкоматтарды пайдаланбаңыз. Банктер мұндай хабарларды орналастырмайды.
- Барлық жағдайларда, мүмкіндігінше, өзіңізге таныс банкоматтарды пайдаланыңыз. Басқа жағдайларда жарық жақсы түсетін және ыңғайлы жерде орналасқан банкоматтарды таңдаңыз.
- Егер Сізарнайы жайда орналасқан банкоматты пайдаланғыңыз келсе, жайдың есігін өз карточкаңызды кіру құрылғысына орналастырып, ашыңыз. Бұл құрылғыПИН-кодты ендіруді талап етпеуі тиіс. Егер Сіз ПИН-кодты ендіруді талап ететін жайға кіру құрылғысын табатын болсаңыз, оны пайдаланбаңыз.
- Сізден кейін кезегін күтіп тұрған адамдар Сіздің ПИН-кодыңызға қарау мүмкіндігінің жоқ екеніне көз жеткізіңіз. ӨзПИН- кодыңызды ендіру кезінде басқалар көрмес үшін банкоматтыңклавиатурасын қолыңызбен жабыңыз.
- Егер сізбанкоматтың дұрыс жұмыс істемей тұрғанын сезетін болсаңыз, «Жою» батырмасын басыңыз, карточаны шығарып алыңыз және басқабанкоматты пайдаланыңыз.
- Карточканы карточкалық слотқа (қабылдау құрылғысының жырығы) салу үшін ешқашан күшті қолданбаңыз.
- Банкоматтың жанында тұрған Сізді ешкімнің алаңдатуына жол бермеңіз.
- Операция аяқталғаннан кейін қолма-қол ақшаны және карточканы алыңыз. Алынған ақшаны банкоматтың жанында қайта санамаңыз – қолма-қол ақшаны, карточканы және чекті бірден алып кетіңіз.
- Егер Сіздің карточкаңыз банкоматта тұрып қалса, осы кезде Сізге көмегін ұсынатын адамдардан сақ болыңыз. Сіздің карточкаңызды оқшаулау үшін бұл жөнінде өз банкіңізге, сондай-ақ, егер банкомат бөлімшеде орналасса, банк бөлімшесінің персоналына дереу хабарлау керек.

2. АЛАЯҚТЫҚТЫҢ НЕҒҰРЛЫМ КЕҢ ТАРАЛҒАН ТҮРЛЕРІ:

Фишинг

Интернет желісін пайдаланушыларға эмитент банктің атынан төлем карточкалары бойынша деректерді нақтылауды өтінген не карточканы ұстаушы кіруі қажет болатын банк сайтына сілтемені қамтитын электронды хаттарды жіберу.
Сайтта оларға жүйенің техникалық іркілісінің салдарынан жоғалған деректерді: кредит карточкасының нөмірін, сәйкестендірушіні, парольді және кейде тіпті ПИН-кодты ендіруді ұсынады. Бұдан кейін төлем карточкасының есебіндегі қаржы қаражаттарын алаяқтар интернет-дүкендер арқылы пайдалануы мүмкін.
Bank RBK Сіздің дербес ақпаратыңызды электронды почта бойынша ЕШҚАШАН СҰРАМАЙДЫ, өйткені бұл қауіпсіздік шараларына қайшы келеді.
Өтінеміз, күдікті операциялар туралы хабарларға назар аударыңыз. Мәселен, егер Сіздің есебіңізге күтпеген ақша түсті деп хабарлайтын болса, алаяқтық әрекетіне күдіктену үшін осының өзі жеткілікті. Егер Сіз алаяқтардың құрбаны болып үлгірсеңіз немесе Сіздің

деректеріңіз бөтен адамдардың қолына түсті деп күдіктенсеңіз, Сізге бұл жөнінде дереу «Bank RBK» АҚ-на хабарлауды ұсынамыз.

Электронды емес фишинг

Бұл «жаңа қызмет» - сауда кәсіпорындарында қолма-қол ақша қаражаттарын алу. Ақша қаражаттарын алуы кезінде ұстаушыдан терілуін эмитент банк тексеруі тиіс болатын өз ПИН-кодыңызды теруді сұрайды. Бірақ ПИН-код эмитентке жіберілмейді, оны алаяқтар ПИН-ПАД-қа ұқсайтын құрылғының көмегімен жазып алады (ПИН-кодтарды теруге және олардың құпиялылығын қамтамасыз етуге арналған сауда терминалының қосымша модулі). Карточканы ұстаушы өз төлем карточкасының шоты бойынша үзінді көшірмеден банкоматтар арқылы өзі жасамаған қолма-қол ақшаны алу операцияларын анықтауы мүмкін.

Скимминг

Банкоматтарға орнату кезінде карточканың деректемелерін де (карточканың нөмірі, арнайы параметрлер), ПИН-кодты да оқуға және жазып алуға мүмкіндік беретін электронды қондырғылардың арнайы түрлері бар. Мұндай құрылғылар банкоматтың әдеттегі бөліктеріне айламен жасырын орнатылады. Оқушы құрал карточканы ендіруге арналған ұяшықтың үстіне, клавиатураның үстіне салынады немесе ақпараттық/жарнамалық кітапшалар жәшігінің астына жасырылған шағын бейнекамералар пайдаланылады.