Улуттук банк маалымдайт

Төлөм системасындагы алдамчылык

Электрондук технологиянын ыкчам өнүгүшү акча которуунун, сактоонун жана төлөмдөр менен эсептешүүлөрдү жүргүзүүнүн улам жаңы формаларынын жаралышына алып келүүдө. Дүйнөлүк тенденцияларга карап биздин республикада да коммерциялык банктардын банкоматтар, терминалдар тармагы менен кызмат көрсөтүүлөрүнүн түрү кеңейе баштады. Банк карталары менен кошо эле мобилдик жана электрондук төлөмдөр, интернет-банкинг кызматы өнүгүүдө. Ошентсе да бардык мезгилде бирөөнүн эсебинен олжолуу болууну каалагандар болгон жана болуп келе жатат. Ал эми алардын курмандыгына айланбоо ар биребиздин билген маалыматыбызга жараша болот эмеспи. Андыктан, төлөм системасындагы алдамчылыкты алдын алуу тууралуу Улуттук банктын Нарын областтык башкармалыгына кайрылып, төмөнкүдөй маалыматтарды ала алдык.

Технология гана эмес, алдамчылык да алдыда

Биздин азыркы жашообузду интернетсиз, уюлдук байланышсыз жана уюлдук аппараттарсыз элестетүү кыйын. Финансы кызматтарын көрсөтүүчү уюмдар дагы бир орунда турбастан, жаңы пайда болгон мүмкүнчүлүктөрдү пайдалануу аракетинде. Эгерде мурда банкка барбай эле төлөмдөрдү аралыктан төлөө мүмкүн эмес көрүнсө, азыр ал жаңылык деле болбой калды, жаңы технологияларды колдонуу менен төлөмдөрдүн улам жаңы түрлөрүн акырындык менен ишке ашырууга мүмкүндүк жаралууда.

Анткени менен тилекке каршы, жаңы технологиялар гана эмес амалын таап, ошол технологиялардан пайда табууну каалагандар да жок эмес. Алдамчылар акча чыгарып алуунун улам жаңы ыкмаларын таап, заманга ылайыкташууда. Адаттагыдай эле андай арам ойлуулардын курмандыгына карапайым жарандар көп учурайт. Буга алардын коопсуздукту сактоонун жөнөкөй эле эрежелерин билбегендиги себепкер.

Алдамчылыктын түрлөрү:

Азыркы учурда эксперттер пластикалык карталарды пайдалануу менен алдамчылык операцияларын ишке ашыруунун негизги түрлөрүн аныкташкан. Алардын айрымдарына токтолсок:

Ак карта же скимминг аркылуу

Карталарды пайдалануу менен алдамчылык операциялардын эң эле кеңири тараган түрлөрүнүн бири - бул мындайча айтканда "ак карталардын" жасалышы же скимминг болуп саналат. Бул үчүн алдамчылар банкоматтарга атайын жазып калуучу жабдууларды орнотушат, ал жабдуулар колдонуучунун картасынын магниттик тилкесиндеги жашыруун маалыматтардын нускасын сактап алат, андан кийин алдамчылар алынган маалыматтардын негизинде, пластиктин кесигине магниттик тилкемесин жасап, уурдалган маалымат жазылган "ак карта" жасайт.

Фишинг аркылуу

Пластикалык карта жөнүндө маалыматтарды колдонуучунун өзүнөн алуу болуп, башкача айтканда фишинг эсептелет. Алдамчылар карта пайдалануучуларга электрондук каттарды жөнөтүшөт, аларда банктын атынан анын коопсуздук системасында келтирилген өзгөрүүлөр жөнүндө билдиришет. Мында алдамчылар ишенгич пайдалануучулардын карта жөнүндө маалыматты жандандыруу максатында пластикалык карталардын номуру, ПИН-коду жазылган жооп-кат же болбосо картаны иштеп чыгарган банктын сайтына кирип атайын анкетаны толтурууну суранышат. Бирок, катта көрсөтүлгөн шилтеме банктын сайтына эмес, окшоштурулган жасалма сайтка алып келет.

Чалуулар аркылуу

Алдамчылар кредит боюнча карыздарын жоюу өтүнүчү менен банктын өкүлдөрүнүн атынан чалууларды уюштурушат. Жаран кредит албагандыгын айтканда, алдамчылар пайдалануучунун пластикалык картасындагы маалыматты тактоону сунуштайт да, кардардын банктык сырдуу маалыматтарына ээлик кылышат.

Интернет аркылуу

Алдамчылыктын кеңири тараган түрү – бул интернет аркылуу жүргүзүлгөн төлөмдөр (ар кандай интернет-сайттар аркылуу төлөө, товар жана кызмат көрсөтүүлөр үчүн акы төлөө ж.б. Мындай операцияларды жүргүзүү үчүн кылмышкерлерге пайдалануучунун атын, картасынын номерин жана иштөө мөөнөтүн билүү жетиштүү, ошондой эле картанын арткы бетинде көрсөтүлгөн кодду киргизүү менен интернет аркылуу төлөмдөрдү жүргүзүүгө болот.

Алдамчылыктан сактануу эрежелери

• Картанын жана ПИН-код жөнүндө маалыматтарын эч кимге көрсөтпөө жана билдирбөө (сиздин тейлөөчү банк сизден телефон аркылуу мындай маалыматты эч качан сурабайт), карта менен бирге ПИН-кодду сактабоо, картанын өзүнө жазбоо керек. Эң мыкты жолу – бул ПИН-кодду эстеп калуу, ошондо жазуу да керек болбойт. ПИН-кодду киргизүү менен болгон операциялар автоматтык түрдө картанын кармоочусу тарабынан тастыкталаарын жана акчаны кайтарып берүүгө мүмкүн болбой тургандыгын унутпоо маанилүү;

• Картаны сиз толук ишенген, бир нече жолу мурда колдонгон, белгилүү корголгон сайттар үчүн гана колдонуңуз;

• Эгерде сиз картаны жоготуп же аны уурдаткан болсоңуз, банктын өзүнө дароо кайрылыңыз, же картада көрсөтүлгөн телефон номерлери боюнча кайрылып, картага бөгөт койдуруңуз. Ошол учурдан тартып, акчанын коопсуздугу үчүн жоопкерчилик банкка арттырылат;

• Интернет аркылуу карта менен төлөөдө ПИН-кодду киргизүүнүн кажети жок экендигин унутпоо зарыл. Операцияны тастыктоо үчүн картанын номерин (картанын алдыңкы бетинде 16 сан) жана текшерүү кодун (картанын арткы бетиндеги сандарды) көрсөтүү гана керек.

Тобокелдиктерди азайтуу үчүн Улуттук банк коммерциялык банктардан жана төлөм системаларынын операторлорунан тутумдун комплекстүү контролун аткаруруу талап кылат. Ошондой эле финансылык сабаттуулугун жогорулатуу боюнча укук коргоо органдарынын, банктардын кызматкерлери жана калк үчүн чоң тажрыйбага ээ болгон эл аралык төлөм системаларынын операторлорун тартуу аркылуу семинарларды өткөрөт.