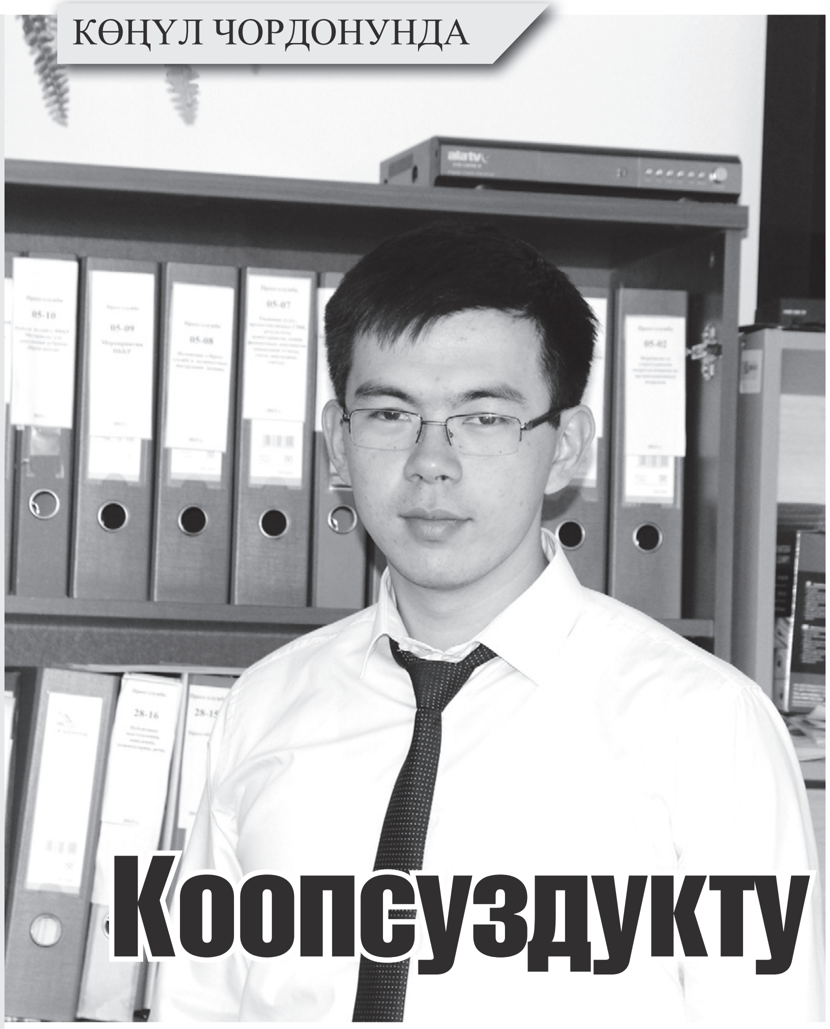
КӨҢҮЛ ЧОРДОНУНДА

Коопсуздукту сактасаң кор болбойсуң

Электрондук технологиянын ыкчам өнүгүшү акча которуунун, сактоонун жана төлөмдөр менен эсептешүүлөрдү жүргүзүүнүн улам жаңы формаларынын жаралышына алып келүүдө. Азыр ири жана орто соода-сервистик ишканалардан товарлар менен кызмат көрсөтүүлөрдү сатып алууда банк карттарын колдонуу эч кимге деле жаңылык эмес. Өнүккөн өлкөлөрдө нак эмес төлөм эбак эле жашоо ыргагына кирген. Дүйнөлүк тенденцияларга карап биздин республикада да коммерциялык банктардын банкоматтар, терминалдар тармагы менен кызмат көрсөтүүлөрүнүн түрү кеңейе баштады. Банк карттары менен кошо эле мобилдик жана электрондук төлөмдөр, интернет-банкинг кызматы өнүгүүдө. Мунун баары өздүк банк эсептерине оңой кирип, аларды интернет аркылуу башкарууга, үйдөн чыкпай эле терминалдар аркылуу эсептерди, сатып алууларды жүргүзүүгө мүмкүндүк берет. Ылдамдык менен ыңгайлуулук, коопсуздук менен ишенимдүүлүк нак эмес төлөмдөрдүн эл арасында өтө популярдуу болушунун негизги себептеринен болду.

Ошентсе да бардык мезгилде бирөөнүн эсебинен олжого туйтунууну каалагандар болгонун эстен чыгарбашыбыз керек. Тилекке каршы, жаңы технологиялар да бул жагынан куру эмес. Алдамчылар акча чыгарып алуунун улам жаңы ыкмаларын таап, заманга ылайыкташууда. Адаттагыдай эле андай арам ойлуулардын курмандыгы да карапайым жарандар. Буга алардын коопсуздукту сактоонун жөнөкөй эле эрежелерин билбегендиги себепкер.

Алдамчылыктын негизги ыкмалары жана андан кантип качуу керектиги тууралуу бизге КРнын Улуттук банкынын Төлөм системаларына көзөмөл жүргүзүү бөлүмүнүн жетектөөчү адиси Улан КУЛМАНБЕТОВ айтып берди.



- Улан мырза, төлөм системасында “алдамчылык” сөзү эмнени түшүндүрөт?

- Төлөм системасында бул термин система кардарларынын же катышуучуларынын банктык эсептеринен акча каражаттарын алуу үчүн банктык жашыруун сыр деп эсептелинген маалыматтарга кирүүгө жана пайдаланууга атайылап жасалган жазгырма аракетти түшүнөбүз. Ошондой эле ички алдамчылык деген бар. Тактап айтканда, алдамчылыкты кардарлардын эсебине кирүү мүмкүнчүлүгү бар болгон банк кызматкерлери өздөрү жасашат (мисалы, маалыматты жайылтуу, жасалмачылык, жашырын маалыматтарды таркатуу). А тышкы алдамчылыкта – мыйзамсыз аракеттер үчүнчү жак тарабынан болот (мисалы, жасалма, уурдалган же жоголгон карттар менен жүргүзүлгөн операциялар, интернет аркылуу товарлар, кызмат көрсөтүүлөр төлөмүндөгү алдамчылык, электрондук жазуучу жабдыкты терминалдарга, банкоматтарга кошуу жана башка). Башкача айтканда, алдамчынын максаты бирөөнүн акчасына түз жана кыйыр ээ болуу.

- Көбүнесе алдамчылыктын кандай ыкмалары кездешет?

- Алдамчылыкты ишке ашыруу ыкмасына карай мобилдик телефондор же СМС жөнөтүүлөр аркылуу алдамчылык, банк карттары жана интернет аркылуу алдоо деп бөлсөк болот. Дүйнө жүзүндө жана бизде мобилдик телефондор же СМС жөнөтүүлөр аркылуу алдамчылык кеңири жайылган. Кыянатчылар ар кандай амалдар менен бирдик жүктөп коюуну өтүнүшөт же таанымал структура же банктын атынан СМС билдирүүлөрдү жөнөтүшөт. Банктык тажрыйбада алсак кылмышкерлер СМС менен же электрондук почта аркылуу банк кардарларына төлөм карттарын блокировкаланып калгандыгы же кардар жөнүндө маалыматтарды жаңыртуу тууралуу билдирүүлөрдү жөнөтүшү мүмкүн. Алдамчылар кийин акылуу болуп чыкчу номерге чалууну же кардарга ыңгайлуу болуш үчүн, банкка келүүгө убакытты кыскартуу үчүн демиш болушуп кардардын өзү тууралуу маалыматтарды, карттардын номерлерин, коддук сөздү жана пинкодду сурашат. Мындай аракет менен алар акчалардын бары-жогун билүүгө, кийин банк эсептерине кирүүгө колдонуш үчүн персоналдык маалыматтарды пин-кодуна чейин алууга тырышышат.

- Алдамчылардын тузагына түшпөш үчүн эмне кылыш керек же эмнени жасоого болбойт?

- Эң негизги эреже – эч кимге, эч качан телефон аркылуу жеке маалыматтарды жана банк картынын номерин (банк картынын алдыңкы бетиндеги 16 цифра), анын иштөө мөөнөтүн, текшерүү кодун (карттын арткы бетиндеги цифраларды) айтпоо керек. Пин-кодду банк кызматкерлерине, укук коргоо жана сот органдарына, ал тургай эң жакын туугандарга да айтпаш керек. Пин-кодду эстеп калуу керек, же аны банктык картадан өзүнчө, көмүскөдө сактоо зарыл. Эгер кимдир бирөө сизге телефон аркылуу банк кызматкери катары чыкса кайра өзүм чалам деп анын аты-жөнүн, кызматын, телефон номерин жазып алыңыз. Андан соң сиздин эсебиңиз ачылган банкка чалып ал жерде ошондой кызматкер иштер иштебесин тактап, анын персоналдык маалыматтарды топтоого укугу бары же жогун жана кандай себеп менен топтоп жатканын аныктаганыңыз оң.. Сиздин банкыңыздын номерлери болсо банктык карттын өзүндө же эсепти ачуу келишиминде көрсөтүлгөн. Эгер алар жаныңызда болбосо банк кабылдамаларынын номерлерин маалыматтык кызматтан же Улуттук банктын www.nbkr.kg электрондук дарегиндеги веб-сайтынан тапсаңыз болот. Бул жерде баары жарандардын кыраакылыгынан жана алардын өздүк, финансылык маалыматтарга карата мамиле кылуу маданиятынан көз каранды.

- Жогоруда айткан төлөм карттарына байланышкан алдамчылдыкты да кенениреэк түшүндүрө кетсеңиз?

- Негизи банк карты коммерциялык банкта ачылган өздүк эсепке алыстан туруп кирүүгө ачкыч болуп эсептелет. Ошондуктан төлөм карттары да кылмышкерлердин бутасына айланат. Кылмыштуу ишке акча уурдоодон баштап интернет-магазиндерди бузуу жана жасалма карт чыгаруу кирет. Бул категорияда банкоматтар менен өзүн өзү тейлөөчү автоматташтырылган терминалдарды манипуляциялоону бөлүп көрсөтсө болот (эл ичинде аларды төлөм терминалы же “кэш-ин” деп коюшат). Манипуляциялоонун негизги максаты банкоматка бекитилген атайын жабдыктын жардамы (скимминг) менен карты тууралуу маалыматтарды жана пин-кодду алуу болуп эсептелинет. Кийинки макалаларыбызда биз буюрса мындай алдамчылык ыкмаларынын ар бирине токтолуп, аларга каршы туруу мүмкүнчүлүктөрү тууралуу айтып беребиз.

- Бизде карттар менен болгон алдамчылык операциялары боюнча кандайдыр бир статистика жүргүзүлөбү? Биздин өлкөдө алдамчылык деңгээли кандай?

- Кыргыз Республикасында банктык карттар менен алдамчылык кылуу деңгээли төмөн. Улуттук банк коммерциялык банктардын отчетторунун негизинде статистика жүргүзүп турат. 2013-жылы 117 төлөм картасын колдонуу менен 142 шектүү транзакция (транзакциялардын жалпы санынын 0,0001 пайызы) катталган. Анын 74 пайызы эл аралык карттарды колдонуу менен жүргүзүлгөн транзакцияларга тиешелүү. Ар бир факт боюнча ички иликтөөлөр жүргүзүлүп, анын 10у боюнча гана карт ээлерисиз акча алуу болгону билинди. Буга коопсуздуктун жөнөкөй эле эрежелерин сактабагандык себепкер болгон. Тактап айтканда, карт үчүнчү жактарга берилген же карта пин-коду менен бир жерде сакталган. А калган жоголгон же уурдалган банк карттары боюнча акча алуу аракеттери өз убагында блокко киргизүү чараларына байланыштуу система аркылуу четке кагылган. Бул жагынан алып караганда акчаны картта сактоонун өтө чоң артыкчылыгы бар. А жасалма карттарды колдонуу боюнча айтсак бир эле факт катталган. Ал карта алынып, банктарга коопсуздук чараларын күчөтүү кабарланган.

- ММКларда Интернет-алдамчылыгы боюнча да көп айтылып жүрөт?

- Интернет-алдамчылыгы да акча жасоого кирет, бирок интернет-сервистердин жардамы менен (электрондук акчаларды алмаштыруучу жасалма акча алмаштыруучулар жана ар кандай төлөмдүк кызмат сервистери, электрондук эсеп колдонуучуларынын персоналдык маалыматтарын бузуп кирүү жана уурдоо жана эсептешүүлөрдө уурдалган маалыматтарды колдонуу). Электрондук эсептешүү системасынын жана интернет-банкингдин өнүгүшү менен алдамчылыктын бул түрү дүйнө жүзүндө барган сайын кеңири жайылып баратат. Кыргыз Республикасында мындай операциялардын жалпы деңгээлин чыгаруу кыйынга турат. Анткени, төлөм кызматтарын тейлегендердин электрондук акча колдонгондугу боюнча маалымат жок. Ошол себептен да колдонуучулардын мындай жагдайлар тууралуу билдирүүгө мүмкүнчүлүгү жок. Коммерциялык банктардын 2013-жылдагы отчету боюнча санкцияланбаган 29 эсептен акча чыгаруу online-сервистердеги эсептешүүлөргө туура келет. Алдамчылыктын алдын алуунун негизги чаралары – текшерилген сайттар менен иштөө. Банк карттары менен электрондук капчыктарды кармоочулар банктардын, төлөм системасынын сунуштаган элементардык коопсуздук эрежелерин сактап, карты жана персоналдык маалыматтарды сактоого этияттык мамиле кылуу керек.

Мелис СОВЕТ уулу

Эң негизги эреже – эч кимге, эч качан телефон аркылуу жеке маалыматтарды жана банк картынын номерин (банк картынын алдыңкы бетиндеги 16 цифра), анын иштөө мөөнөтүн, текшерүү кодун (карттын арткы бетиндеги цифраларды) айтпоо керек. Пин-кодду банк кызматкерлерине, укук коргоо жана сот органдарына, ал тургай эң жакын туугандарга да айтпаш керек. Пин-кодду эстеп калуу керек, же аны банктык картадан өзүнчө, көмүскөдө сактоо зарыл. Эгер кимдир бирөө сизге телефон аркылуу банк кызматкери катары чыкса кайра өзүм чалам деп анын аты-жөнүн, кызматын, телефон номерин жазып алыңыз.