ТӨЛӨМ СИСТЕМАСЫНДАГЫ АЛДАМЧЫЛЫК ЖАНА АНЫ МЕНЕН КҮРӨШҮҮ

Электрондук технологиянын ыкчам өнүгүшү акча которуунун, сактоонун жана төлөмдөр менен эсептешүүлөрдү жүргүзүүнүн улам жаңы формаларынын жаралышына алып келүүдө. Учурда ири жана орто соода-сервистик ишканалардан товар сатып алууда жана кызмат көрсөтүүлөрдү төлөөдө банк карталарын колдонуу эч кимге деле жаңылык эмес. Өнүккөн өлкөлөрдө накталай эмес төлөм эбак эле жашоо нормасы болуп калган. Дүйнөлүк тенденцияларга карап биздин өлкөдө 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. 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 накталай 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 Кыргыз Республикасынын 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 пайдалануура 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, жашыруун маалыматтарды таркатуу)*. Ал эми тышкы алдамчылыкта – мыйзамсыз аракеттер үчүнчү жак тарабынан болот *(мисалы, жасалма, уурдалган же жоголгон карталар 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 кездешип жүрөт?

– Алдамчылыкты ишке ашыруу ыкмасына карай уюлдук телефондор же СМС жөнөтүүлөр аркылуу алдамчылык, банк карталары жана интернет аркылуу алдоо деп бөлсөк болот. Мындан тышкары акча которуу системаларын колдонууда финансылык тобокелчиликтерге кезигүү мүмкүн. Сактануу үчүн коопсуздук чараларын сактоо зарыл. Дүйнө жүзүндө жана бизде уюлдук телефондор же СМС жөнөтүүлөр аркылуу социалдык инженерия деп аталган алдамчылык кеңири жайылган. Кыянатчылар ар кандай амалдар менен бирдик жүктөп коюуну өтүнүшөт же таанымал фирма же банктын атынан СМС билдирүүлөрдү жөнөтүшөт. Банктык тажрыйбада алсак, кылмышкерлер СМС же электрондук почта аркылуу банк кардарларына төлөм карталарынын 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 коротпоо үчүн демиш болуп кардардын өзү тууралуу маалыматтарды, карталардын номерлерин, коддук сөздү жана пин-кодду 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 кылуу керек же эмне кылбоо керек?

– Эң негизги ереже – эч кимге, эч качан телефон аркылуу жеке маалыматтарды жана банк картасынын номерин *(банк картасынын алдыңкы бетиндеги 16 цифра)*, анын иштөө мөөнөтүн, текшерүү кодун *(картанын арткы бетиндеги цифралар)* 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 иштеиштебесин тактап, анын персоналдык маалыматтарды топтоого укугу бар же жогун жана кандай себеп менен топтоп жатканын аныктаңыз. Сиздин банкыңыздын телефон номерлери банктык картанын өзүндө же эсепти ачуу келишиминде көрсөтүлгөн. Эгер алар жаныңызда болбосо банк кабылдамаларынын номерлерин маалыматтык кызматтан же Улуттук банктын **www.nbkr.kg** электрондук дарегиндеги вебсайтынан тапсаңыз болот. Бул жерде баары жарандардын кыраакылыгынан жана алардын өздүк, финансылык маалыматтарга карата мамиле кылуу маданиятынан көз каранды.

– Жогоруда айтып кеткен төлөм карталарына байланышкан алдамчылыкты да кененирээк түшүндүрө кетсеңиз?

– Негизи банк картасы коммерциялык банкта ачылган өздүк эсепке алыстан туруп кирүүгө ачкыч болуп эсептелет. Ошондуктан төлөм карталары да кылмышкерлердин бутасына айланат. Кылмыштуу ишке акча уурдоодон баштап интернет-магазиндерди бузуу жана жасалма карталарды 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 карта 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.

– 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 өнүгүшү менен алдамчылыктын бул түрү дүйнө жүзүндө барган сайын кеңири жайылып баратат. Кыргызстанда 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. Алдамчылыкты алдын алуунун негизги чаралары – текшерилген сайттар менен иштөө. Банк карталарын жана электрондук капчыктарды кармоочулар коопсуздуктун банк, төлөм системасы сунуштаган элементардык эрежелерди сактап, картаны жана персоналдык маалыматты сактоого этияттык мамиле кылуу керек.

– Сиз акча которуу системаларын колдонуудагы тобокелчиликтерге кезигүү мүмкүнчүлүгү жөнүндө айттыңыз. Сактануу үчүн кандай чараларды көрүү керек?

– Акча которуу системаларын колдонууда митаамчылыкка каршы төмөнкү алдын ала сактануу чараларын көрүү зарыл:

- ✓ Акчаны жөнөтөрдө алуучунун аты-жөнүнүн тууралыгын тактагыла.
- ✓ Жөнөтүлүү акчанын суммасын, алуучунун реквизитин, банктык эсептин номерин жана башкаларын дыкат текшергиле.
- ✓ Алуучудан башка эч кимге контролдук номерди айтпагыла.
- ✓ Акчаны аларда жөнөтүүчүдөн акчанын суммасын, контролдук номерди жана сизге акча салган акча которуу системасын тактаңыз.
- ✓ Мүмкүнчүлүккө жараша алдамчылык болбош үчүн акчаны тааныш адамдарга гана которгула.
- ✓ Банктан алган акча каражатын которуу тууралуу документтин сканерден өткөрүлгөн көчүрмөсүн эч кимге жөнөтпөгүлө.
- ✓ Эгер кайсы бир товарды же кызматты сатып алып жатканда сатуучу акчаны жакын туугандарыңыздын же өзүңүздүн атыңызга которуп, андан соң сиздин төлөө мүмкүнчүлүгүңүздү бышыктоо максатында төлөм документинин сканердик көчүрмөсүн ага жөнөтүүнү сураса, ал товарды сатып алуудан баш тартыңыз, балким, бул алдоо болуп калышы ыктымал. Учурда алдамчылар ушунчалык өнүккөндүктөн жасалма документ менен акча которуу системасы аркылуу жөнөтүлгөн акчаны чыгарып алышы мүмкүн. Эгер тааныш эмес сатуучулар товар, кызмат төлөмү үчүн акчаны акча которуу системасы боюнча которууну сураса, акчаны алардын эсебине түз которууну сунуштаганга аракет кылгыла. Эгер сатуучу макул болбосо, анда сизди алдаганга аракет кылып жатышы толук ыктымал.

Ибрагим Жусуев