КИБЕРКЫЛМЫШТУУЛУКТАН САКТАНА БИЛИҢИЗ!

Инновациялык технологиянын күн санап өнүгүп жатышы бизнести алып барууда да революциялык өзгөрүштөрдү жаратып жатат. Ошондуктан турмушубузда нак эмес төлөм менен интернет аркылуу чет өлкөдө соода-сатык жүргүзүүгө шарт түзүлдү. Электрондук төлөм калк арасында кеңири таркап, азыр элет жергесинде да жарандарыбыз банк карталарды колдонуп жаткан кез. Ал ылдам жана ыңгайлуулугу менен өзгөчөлөнөт. Бирок криминалдык дүйнө дагы өз ордунда туруп калган жок, бирөөнүн каражатын кымырып алуунун көптөгөн жолдору пайда болууда. Мындай ыплас жол менен алектенүүнү КИБЕРКЫЛМЫШТУУЛУК деп атап жүрүшөт. Кыргызстандын банк тармагындагы киберкылмыштуулук тууралуу Кыргыз Республикасынын Улуттук Банкынын Инспекциялоо башкармалыгынын айрым операцияларга экспертиза жүргүзүү бөлүмүнүн башкы инспектору БАКЫТ ДАЙЫРОВ менен маектештик.

– Саламатсызбы?! Алгач киберкылмыштуулук тууралуу айта кетсеңиз. Мындай кылмыш кантип онүгүүдо?

— Саламатчылык! Дүйнөдө сервистик кызмат көрсөткөн компаниялар виртуалдык ишмердүүлүк сунуштап, “оффлайн” деп аталган сервис өнүгүп баштады. Кадимки эле соода-сатыкты үйдөн чыкпастан мобилдик технологиянын жардамы менен жүргүзүү адатка айланууда. Башкача айтканда, айлана-чөйрөдөгү буюмдар аралыкта башкарылып, “акылдуу” болуп баратат. Бирок бул күнүмдүк жана көнүмүш кызмат көрсөтүүгө акырындык менен киберкылмыштуулук аралашып жатканы көйгөй жаратууда. Медалдын эки тарабы болгон сыяктуу эле мыйзамга баш ийген атуулдар менен катар криминалдык элементтер да жок эмес. Азыркы учурда киберкылмыштуулук заманбап дүйнөгө олуттуу коркунуч туудурган жана бат өнүгүп келе жаткан кылмыш болуп калды. Анткени кибермейкиндиктеги кылмыштуулук өз алдынча гана коркунуч жаратпастан, азыркы турмушта кадимки кылмышты ишке ашыруучу криминалдык ишмердүүлүк болуу менен бирге далилдик базанын чогулушун белгилүү деңгээлде татаалдантууда.

– Киберкылмыштуулук кандайча ишке ашырылат жана бул боюнча статистикалык маалыматтар барбы?

— Бүткүл дүйнөлүк түйүн эсептелген интернет – маалымат алуу жана маалымат алмашуу боюнча элге кеңири кучагын ачуу менен бирге кылмыштуулук максатта илим менен техниканы пайдалангандарга да шарт түзүп жатат. Күн сайын 100дөн ашуун зыяндуу программанын түрү иштелип чыгат. Стратегиялык жана эл аралык изилдөө борборунун *(Center for Strategic and International Studies)* маалыматына таянсак, 2014-жылдын жыйынтыгы боюнча киберкылмыштуулук бүткүл дүйнөдө 400 миллиард доллардан ашуун экономикалык чыгымга учуратып, 300 миллионго жакын адамдын жеке маалыматы киберкылмышкерлер тарабынан уурдалып кеткен. Тилекке каршы, мындай өлкөлөрдүн арасында Кыргызстан да бар.

– Кыргызстанда кайсы банктык продуктулар киберкылмыштуулук коркунучун туудурат?

— Өлкөбүздүн банк системинде да мобилдик капчык, электрондук акча, мобилдик банкинг, интернет банкинг жана башка ушул сыяктуу заманбап банк продуктулары кылмышкерлер тарабынан чабуулга алына баштады. Ошондуктан биздин алдыбызда учурда жаралып жаткан коркунучтардан коргонуу максаты турат. “CITRIX” компаниясынын

“Киберкоркунучтарга каршы күрөш тууралуу” отчётуна ылайык, көбүнчө корголбогон тармак катары социалдык түйүндөрдөгү мобилдик технологиялар жана киберкылмышкерлер эсептелсе, кылмыштуулуктун саны көбүнчө жеке маалыматтарды уурдоодо кездешет экен. Тажрыйба көрсөткөндөй, тийиштүү деңгээлдеги коопсуздук системиндеги эң эле корголбогон звено болуп акыркы колдонуучу эсептелет. Катачылыктар кеткенине карабай же кызмат көрсөтүүчү адистер тарабынан аткарылган көз боёмочулуктун болушу, эң негизгиси ошол кызматтан колдонуучунун өзүнүн жоопкерчилигине жараша болот. Кызмат көрсөтүү боюнча системде кабыл алынган бардык алдын алуучу иш-аракеттер бир эле убакыттын ичинде колдонуучунун коопсуздук негиздерге тоготпостук мамиле жасоосунун натыйжасында жокко чыгышы мүмкүн.

– Бул кылмыштын түрү көбүнчө кандай жол менен ишке ашырылышы мүмкүн?

— Бүгүнкү күндөгү эң көп жана жөнөкөй жол менен кездешкен кылмыштын түрү кадимки мобилдик каражаттар аркылуу ишке ашырылууда. Ал персоналдык маалыматтарды, сыр сөздү *(пароль)* же кодду алуу максатында СМС билдирүү, телефон чалуу же почта аркылуу жүргүзүлөт. Ниети бузук адамдар төлөм уюмунун, банктын адиси катары өзүн тааныштырып, атуулдардын ишенимине киришет да, купуя маалыматтарды алышат. Андан кийин кылмышкер ал маалыматтарды пайдаланып, курмандыкка учураган адамдын акча каражатына жетет.

Бир кыйла техникалык жактан татаал жана оор деп "фишинг" эсептелет. Мында кылмыш атайын зыян келтирүүчү программанын, техникалык жабдуулардын жана системдин алсыздыгынын жардамы менен ишке ашырылат. Аны массалык түрдө почта аркылуу банктын атынан потенциалдуу курмандыкка жиберип, “аткарылуучу” файлды *(зыянкеч программа)* ачууга мажбурлашат же жалган сайтка которушат. Кылмышкерлер колдонуучулардын персоналдуу маалыматын алуу максатында түп нускасынан айырмаланбагандай сайттын кудум көчүрмөсүн түзүшөт. Ал эми курмандыкка чалынган жаран эч нерседен шек санабай сайттын көчүрмөсүндө жүргөндүгүн билбестен өзүнүн персоналдык маалыматтарын, сыр сөзүн жана кодун кылмышкерге беришет.

Дагы бир кеңири жайылтылган ыкма – бул "скимминг". Анда атайын жабдуу банкоматтын слотуна тиркелет да, картадагы маалыматтардын баарынын мазмунун окуп чыгат. Миниатюралык видеокамеранын жардамы менен же клавиатурадагы атайын тиркемелер аркылуу пин-код эсепке алынат. Маалыматтын баары алынгандан кийин жасалма карта даярдалып, банкоматтан нак акчаны чыгарып алуу ишке ашырылат. Бул иш көбүнчө башка шаарда же өлкөлөрдө аткарылат.

– Жеке жактар гана эмес ири банктар менен финансылык институттар дагы киберкылмышкерлердин курмандыгы болушу мүмкүнбү? Эгер болсо, анда ал кандайча ишке ашат?

— Учурдагы жаңы муундагы кылмышкерлер технологиянын өзгөрүшүнө бир кыйла оперативдүү жана тездик менен таасир этет. Топ-топ болуп биригип алып, өздөрүнүн билимдерин, тажрыйбаларын жана ири финансылык ресурстарын чындашат. Ал эми банктар бул учурда маалыматтан артта калып, куугундун ролун аткарып калышат. Тилекке каршы, киберкылмыштуулук тармагындагы күрөштө кезектеги сокку кайдан келерин билүү мүмкүн эмес. Анткени жаңы технологиянын жаңы алсыз жагы кайсында жатканын алдын ала билүү кыйын. Ал эми маалыматтык коопсуздукту коргоонун классикалык каражатын колдонуу кылмыштын алдын алууда жетишсиздик кылат. Ошондуктан киберкылмыштуулукка каршы күрөшүү боюнча конкреттүү бир иш-чараларды кабыл алуу кыйынчылыкты жаратат. Эң негизгиси кибертармактын тышкы индикаторун көзөмөлгө алып, өз убагында пландоо жана киберкылмыштуулукка каршы иш-чараларды жайылтуу керек.

– Алдамчылардын тузагына чалынбаш үчүн эмне кылуу керек?

— Биринчиден электрондук акчага карата мамиле нак акчага жасагандай эле коопсуз болушу шартталат. Эң негизгиси интернет банкинг, мобилдик-банкинг жана электрондук капчыкты колдонуу боюнча коопсуздук чараларды жакшы билүү керек. Тобокелдикти төмөндөтө турган эң жөнөкөй кеңештер булар:

- Интернет банкингди колдонуп товарга же кызмат көрсөтүү үчүн коомчулук колдонгон компьютерден же интернет-кафеден төлөм жүргүзүүгө болбойт;
- Электрондук төлөмдү күмөн санаткан же бейтааныш интернет түйүндөн жүргүзүү кооптуу;
- Сөзсүз браузердеги сайттын дарегин жакшылап текшерүү керек *(бир эле символу туура эмес болушу жасалма сайт экендигинен кабар берет)*;
- Лицензияланган антивирустук камсыздоо программасын киргизүү жана аны үзгүлтүксүз жаңылап туруу;
- Ар түрдүү мобилдик тиркемелерди *(оюн, программа ж.б.)* бир гана расмий сайттардан жана булактардан көчүрүү;
- Күмөн санаткан сайттарга кирбөө жана белгисиз жактардын билдирүүлөрүн ачпоо сунушталат.

Ал эми банкомат кызматынан колдонууда:

- Тийиштүү операцияны жүргүзүү алдында банкоматтын сырткы көрүнүшү менен клавиатурада жат көрүнүш жок экендигине көңүл бурунуз;
- Эч качан эч кимге өздүк пин-кодду айтпаңыз *(банк кызматкери болсо дагы)*;
- Эгерде тийиштүү операциядан кийин сиздин карточка кайтарылбай калса, дароо өзүңүздүн банкыңызга кайрылыңыз;
- Мүмкүн болсо өз карточкаңызга бир күндүк лимит жана башка чектөөлөрдү киргизип коюңуз.

Эң негизгиси толугу менен киберкылмыштуулуктан арылуу башка кылмыштын түрлөрү сыяктуу эле мүмкүн эмес экенин эстен чыгарбоо зарыл. Башкысы – бул процессти технологиянын өнүгүшү менен тийиштүү талаптарга ылайык көзөмөлдөөгө болот.

Ибрагим Жусуев