6. Копылов В.А. Информационное право. –М.: Юрист, 2002. – 612с.
7. Конвенция об обеспечении международной информационной безопасности (концепция) – Электронный ресурс – [Режим доступа] — http://www.scrf.gov.ru/documents/6/112.html.
8. Data Protection Act 1998 – Электронный ресурс – [Режим доступа] - https://www.legislation.gov.uk/ukpga/1998/36/contents.
9. Жарова А.К. Опыт правового обеспечения безопасности персональных данных в Великобритании // Государство и право. – 2017. -№6. –С.70-79.
10. Приоритеты национальной безопасности в условиях глобализации. / Жатканбаев Е.Б. и др.- Алматы: Қазақ университеті, 2006. -329с.
11. Мовкебаева К.А., Карманов А. Информационные операции США в контексте обеспечения кибербезопасности //Вестник КазНУ. Серия м.о. и м.п. -2016.-№2. –С.236-242.
12. Строева Ю. О. Информационная безопасность детей в телекоммуникационных сетях // Молодой ученый. — 2017. — №50.1. — С. 41-43. — URL https://moluch.ru/archive/184/47336/.
13. Танекова М.О. К вопросу о распространении порнографических материалов в социальных сетях // Вестник КазНУ. Серия м.о. и м.п.- 2016. - №4. –С.158-164.
14. Нормативное постановление Верховного Суда Республики Казахстан от 8 декабря 2017 года №11 «О некоторых вопросах судебной практики по применению законодательства о террористических и экстремистских преступлениях» – Электронный ресурс – [Режим доступа]- https://online.zakon.kz/Document/?doc_id=355366.
15. Государственная программа «Цифровой Казахстан». Утверждена Постановлением Правительства Республики Казахстан № 827 12 декабря 2017 года. – Электронный ресурс – [Режим доступа]- https://zerde.gov.kz/activity/management-programs/the-state-program-d.

Амангелдинова З.Ж., Тәңірберген С.С., академик Е.А.Бөкетов атындағы Қарағанды мемлекеттік университеті, экономика факультеті, топ. Фн-21, студенттер
(Ғылыми жетекші – э.ғ.м., аға оқытушы Топшахова Г.Р.)

ТӨЛЕМ КАРТАЛАРЫНА ҚАТЫСТЫ АЛАЯҚТЫҚ МӘСЕЛЕЛЕРІН ШЕШУ ЖОЛДАРЫ

Қазіргі уақытта төлем карточкалары қаржы құралдарының арасында төлем жүйелерінің ең көп бөлігін қамитиды . Алайда бұл қаржылық құралдың өзіне тән кемшіліктері де аз емес оның ішінде осы құралдар арқылы жасалатын түрлі алаяқтық әрекеттер.Карточкалық алаяқтықтың біріншіжәне қазіргі кезде ең көп таралған түрі - «ақ карталар» немесе «клон карталары» деп аталатын карталар жасау. Алаяқтар пайдаланушының картасының магниттік жолағындағы құпия ақпаратты оқиды, содан кейін магниттік жолағы бар пластиктен және ұрланған ақпараттан «ақ карточкалар» жасайды. Осыдан кейін, шабуылдаушылар қолданыстағы картаның иесінің шотын еркін қолдана алады, бұл жағдайда олардың «бөтен» төлемдерге қатыспайтындығын дәлелдеу өте қиын болады.

Картада сақталған құпия ақпаратты оқу әр түрлі жолмен жасалуы мүмкін. Олардың ішіндегі ең көп тарағаны - алаяқтардың дүкендер, қонақүйлер, мейрамханалар және басқа да сауда-ойын-сауық кәсіпорындарының қызметкерлерімен жасырын келіссөздері. Мұндай қастандықтың нәтижесі - қылмыстық құрылымдардың өкілдеріне карточкалардың деректемелері туралы ақпаратты беру. Карта алаяқтардың қолында болса, төлем картасы арнайы құрылғы (скиммер) арқылы өтіп, оның магниттік жолағында сақталған мәліметтерді скимминг арқылы оқи алады. Осылайша, алаяқтар картаның маңызды ақпараттарын аладыжәне оған қажетті соманы енгізерде, қол қою қажет болмайды, ал операция үшін барлық есептерді картаның заңды иесіне бағыттайды.

Қылмыстық құрылымдар өздерінің сауда дүкендерін құруда.Осындай «сауда нүктелерінің» мақсаты қарапайым - клиенттердің пластикалық карталары туралы мүмкіндігінше көп ақпарат алу. Алаяқтар Интернет-сайттарды бұл үшінжиі пайдаланады. Осындай сайттың қызметін бір рет пайдаланып (мысалы, тауарды сатып алған немесе бейне роликті жүктеп алған), карта иесі оның жазылушысы болғанын таң қаларлық түрде анықтайды және осылайша, ай сайын жазылым үшін төлем алынып отырады , одан бас тарту қиын болады.

Карточкалық алаяқтықтың тағы бір түрі фишинг деп аталады. Ол қолданушыдан пластикалық карта туралы мәліметтерді алады. Зиянкестер қолданушыларға өзінің қауіпсіздік жүйесінде болған өзгерістер туралы банктің атынан есеп беретін электрондық пошталарды жібереді. Сонымен бірге, алаяқтар сенімсіз пайдаланушылардан карточка туралы ақпаратты,

оның ішінде «несие картасы» нөмірін және оның PIN-кодын көрсетіп, жауап хатын жолдау арқылы немесе эмитент банктің веб-сайтына кіріп, тиісті нысанды толтыру арқылы сұрайды. Алайда, хатқа қосылған сілтеме банктің ресурстарына емес, осы жұмысты имитациялайтын жалған веб-сайтқа жібереді.

Бұл құқық бұзушылық қоңыраулар азаматтардың ұялы телефондарына банктің өкілдеріретінде несие берешегін өтеу туралы хабарлайды.Азамат несие алмағаны туралы айтқан кезде, оның пластикалық картасының егжей-тегжейін нақтылауды сұрайды. Кейіннен бұл ақпарат пайдаланушының карт-шотынан рұқсат етілмеген ақша аударымдарын алу үшін пайдаланылады.

Өз ақшаңызды сақтау үшін есіңізде болсын: банктер мен төлем жүйелері ешқашан хаттар жібермейді және клиенттердің телефондарына олар туралы мәліметтер ұсынуды сұрамайды. Егер мұндай жағдай туындаса, сізден банкке жеке келуіңіз сұралады.

Пластикалық картаның алаяқтық ықтималдығын төмендетудің жалғыз нақты әдісі - қарапайым қауіпсіздік ережелерін сақтау. Банк қызметкерлері өз клиенттерін карточкаларына көбірек көңіл бөлуге шақырады: карточкаларды үшінші тұлғаларға сеніп тапсырмау, оларды қараусыз қалдырмау, оңай қол жетімді жерлерде ПИН-кодты жазып алмау, тіпті картаның өзіне. Картаны алғаннан кейін бірден оның артқы жағына қолтаңбаңыздың үлгісін қалдырыңыз. ПИН-кодты ешқашан ешкімге айтпаңыз. Карточканы шығарған банк қызметкерлері де, банкомат қызметкерлері де оны талап етуге құқылы емес.

Мейрамханаларда немесе дүкендерде төлем жасағанда картаны жоғалтпаңыз. Нақтырақ айтсақ, картаңызды сіздің импринтеріңізден өткізуді сұраңыз. Сіздің картаңызбен не істеп жатқанын мұқият қарап шығыңыз, күмәнді мекемелерде несие картасымен төлемеңіз және түбіртектеріңіздің көшірмелерін сақтаңыз. Мейрамханада қызмет көрсетуге ақы төлеу кезінде, карта иесінің көзінен тыс болғанда, тек бірнеше минут ішінде картаның магниттік жолағынан оның иесі және карточкалық шоттағы қаражат сомасы туралы құпия ақпарат оқылған жағдайлар жиі кездеседі.

Сіздің картаңыздағы ақша қозғалысын тексеріңіз. Құқық бұзылған жағдайда карточка иесі қатаң келісілген шарттарда көрсетілгендей іс-шаралар қолдана алады. Картаны пайдаланған шоттар бойынша операцияларға ерекше назар аудару керек.

Банк қауіпсіздігі жөніндегі мамандардың өз клиенттеріне беретін соңғы кеңесі - төлем картасының жоғалуы немесе ұрланғаны туралы банкке дереу хабарлау. Қылмысты іздеуде тергеу екі аптадан кейін немесе ұмытылып қалған жағдайда қылмысты анықтау қиын болады.

Интернетте картамен төлеу кезіндегі қауіпсіздік шараларылары:

- Өзіңіз туралы және сіздің картаңыз туралы мәліметтерді таныс емес, білмейтін сайттарға қалдырмаңыз. Достарыңыз бен таныстарыңыздан осы сайттар туралы сұраңыз, тиісті конференцияларға қызығушылық танытыңыз, сіз ақша аударымдарын жасайтын ұйымның қайда екенін біліңіз. Сонымен қатар, осы веб-сайт арқылы елді мекендердің қауіпсіздігін растайтын әртүрлі куәліктерге назар аударыңыз. Егер мекенжай мүлде болмаса немесе ол сенім тудырмаса, төлем жасамас бұрын, оны жасаудың қажеті туралы ойланыңыз.

- Интернетте үлкен ақшаға ие карталарды пайдаланбаңыз. Осындай мақсаттар үшін жеке карта алып, қажет болған жағдайда ақша аударған дұрыс.

- Сіздің шотыңыздан ақшаны заңсыз алып тастау туралы кішкене күдік туындаған жағдайда, банкке хабарласыңыз. Карточка иесінің карточкалық шоттан ақшаны заңсыз есептен шығарудан бас тарту немесе оған қарсы шығу үшін белгілі бір мерзім бар. Бұл кезеңнің ұзақтығы картаны шығарған банкте нақтылануы керек.

Электронды қаржылық алаяқтықтың тағы бір тәсілі-бұл банкоматтар арқылы карточка туралы деректерді алу үшін арнайы техникалық құралдарды пайдалану. Ол үшін, атап айтқанда, банкоматтың пернетақтасына ерекше "жапсырмалар" пайдаланылады, олар карточка иесі қаражатты алып жатқанда, пернелерді басқан кезде есте сақтайды.

Тағы бір құрылғы - бұл пластикалық конверттер, олардың мөлшері карта өлшемінен сәл үлкен. Олар банкомат карталарын оқу құрылғысының саңылауына салынған. Банкомат, әдетте, магниттік жолақтағы деректерді оқи алмайды, бірақ конверттің дизайнына байланысты картаны қайтару мүмкін емес. Осы уақытта шабуылдаушы келіп, өз көмегін ұсынады, бірақ ол үшін картаның иесі бірнеше әрекеттерді, соның ішінде PIN-кодты теруі керек. Осыған қарамастан, карта қайтарылмайды. Егер иесі эмитент-банкке жүгінуге кетсе, алаяқ конвертті несиелік картамен бірге жайлап шығарады. Ол PIN-кодты бұрыннан біледі және ол тек шоттан ақша ала алады.

Картоқабылдағышқа тек конверттер ғана емес, сонымен қатар заңды пайдаланушы қаражатты алып тастағанда, карточкадан ақпаратты оқитын скимерлер негізіндегі арнайы құрылғылар да кірістірілуі мүмкін.

Банкоматтарда микро камера жиі орнатылады. Ол PIN-кодты терген адамды тіркейді және теру деректерін алаяқтарға береді.

Тағы бір құрал - бұл жалған банкоматтар. Олар карточкадағы ақпаратты, оның ішінде PIN-кодты дұрыс оқиды, бірақ ақша бермейді. Карточка иесіне қайтарылады, бірақ ол туралы барлық ақпарат «банкоматтың» жадында сақталады.Бұл әдіс өте қымбат және оны тек ірі қылмыстық топтар қолданады.

Банкоматтағы қауіпсіздік техникалары:

Біріншіден, банкоматтарды адам саны аз жерлерде немесе адамдар көп жиналатын жерлерде пайдаланбауға тырысыңыз. Адам саны аз жерде ақшаны алу кезінде карточка иесін тонау тым осал объект болады. Ал адам көп жерде пайдаланушы енгізген ПИН-кодты ешкім көрмейтініне сенімді бола алмайды.

Екіншіден, сіз енгізген ПИН-кодты бөгде адамдарға көруге мүмкіндік бермеңіз. Банкоматтың басқа пернетақтасын жабудан ұялмаңыз. Және мүмкіндігінше ПИН-кодты енгізгенде қателеспеңіз. Үш қате кодты енгізгеннен кейін банкомат картаны кідіртеді.

Үшіншіден, барлығы банкоматтан алынғанын тексеріңіз. Операция аяқталғаннан кейін карточка иесінде : карточка, ақша және жүргізілген операция туралы көшірме қалуы тиіс. Егер бір нәрсе жетіспесе, ал банкомат ешқандай қосымша ақпарат хабарламаса, онда бұл жерде бір шикіліктің бар болуы мүмкін және карточка иесі алаяқтардың құрбаны болу қаупі бар.

Төртіншіден, банкомат беретін операция қорытындысы бойынша көшірмелерді әрдайым сақтаңыз. Бұл сізге шығыстардың есебін жүргізуге және шоттан ақшаны есептен шығаруды бақылауға мүмкіндік береді [1].

Пластикалық карталардан ақшаны ұрлаудың мынадай бірнеше әдістері бар:

Сіздің пластикалық картаңыздан ақша алу үшін, сіздің карта нөмірін және CVS (картаның кері жағындағы Соңғы үш сан) білу жеткілікті. Бұл деректерді алаяқтар қалай біледі? Иә, өте оңай, адамдар өздері айтып береді.Негізінде, алаяқтар құрбандарынан карта деректерін алып тастаудың үш-төрт әдісін қолданады.

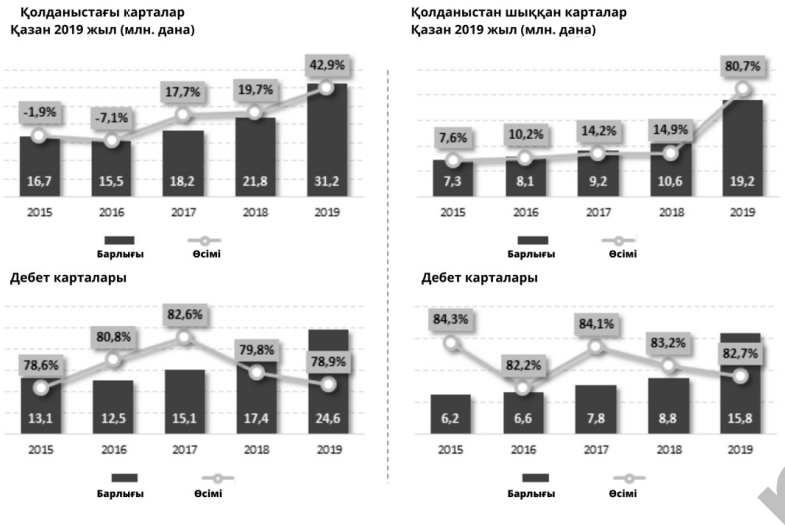
Бірінші әдіс. Телефоныңызға сіз ноутбукты ұтып алғаныңыз туралы және ұялы телефонның екінші шетінде осы нөмірге қоңырау шалған кезде ұтысты алу үшін қайта қоңырау шалуды сұрайтын SMS келеді .Олар оған ноутбуктің құнын оның пластикалық картасына жіберуді ұсынады және бұл үшін картаның нөмірі керектігін айтады. Құрбан осы деректерді хабарлаған кезде картасындығы барлық ақшалармен қоштасады.

Сізде Банк жіберетін барлық смс-тің кері телефоны жоқ, тек идентификаторы бар екенін ескеріңіз, яғни телефонда «кімнен»екені және банктің атауы көрсетіледі.

Екінші әдіс. Бұл жағдайда да телефонға SMS келеді, бірақ сіздің картаңыз бұғатталғанын және кері қоңырау шалуыңызды сұрайды.Мұнда жәбірленушіге жақын орналасқан терминалға немесе банкоматқа барып, кассирдің нөмірін және құлыптан босату нөмірін енгізіп, сонымен қатар ұялы операторды таңдау ұсынылады [2].

Бұл біздің елде қандай аңқау адамдар бар екенін дәлелдейтін жағдайлардың бірі, өйткені жәбірленуші кассаның нөмірінің орнына ұялы байланыс операторын таңдайды, соманы енгізеді, содан кейін алаяққартаны салып, ұялы телефонына төлемді төлеуін сұрайды. Есіңізде болсын, ақша телефонға интернеттен аударылады, бұл жағдайда алаяқ бірден оны ұялы телефоннан кейбір электрондық әмиянға аударады. Әрине, SIM-карталар мен электрондық әмияндар үшінші тарапқа тіркелген. Мұндай жағдайларда ақшаны қайтару қазірдің өзінде мүмкін емес болады.

ҚР өңірлерінің арасында дәстүрлі түрде дебеттік карточкалардың ең көп саны Алматыда есептеледі: 5 млн-нан сәл артық, оның 3,2 млн-ы белсенді. Екінші орында Түркістан облысы мен Шымкент: 2,7 млн дебеттік карточка, оның ішінде пайдаланылған-1,7 млн. көшбасшылар үштігіне Нұр-сұлтан: 2,6 млн дебеттік карта, оның ішінде белсенді - 1,6 млн. Еліміздегі кейбір карта пайдаланушылар алаяқтарға жем болуы мүмкін, карталар санының өсуіне байланысты.



Сурет 1. ҚР карталар бойынша ақпарат, 2019 жыл [3]

Банк картасын ұрылардан қорғау шаралары:

Банк карталарының кең таралуы шоттан қаражат ұрлауға бағытталған әртүрлі айлалардың көптеп пайда болуымен қатар жүреді. Мамандар өздерін ұрлықтан қалай қорғау жөнінде бірқатар ұсыныстар берді:

- Ең алдымен, банк карталарына жеке ақшалар сияқты қарап, оны қауіпсіздікте сақтау керек. Картаны қараусыз қалдырмау керек, өйткені алаяқтарға қаражатты аудару, барлық қажетті ақпаратты көшіру үшін санаулы секунд жеткілікті. Айтпақшы, сол себепті картаны үшінші тұлғаларға, соның ішінде туған-туысқандар мен жақындарына беруге болмайды. Олар үшін көптеген банктер қосымша карталар шығарады. Егер ұрлық жасалса, дереу қолдау қызметіне барып, картаны бұғаттау керек.

- Ұсынымдардың келесі бөлігі алаяқтардың ұрлық үшін жиі пайдаланатын банкоматтарды пайдалануға қатысты. Терминалға келген сайын оны құрылғының жалпы құрылымынан шыққан күдікті заттардың бар-жоғын тексеру керек. Құрылғының қауіпсіздігіне көз жеткізгеннен кейін, пинкодты енгізу ұсынылады, әрқашан сандарды бөгде көзден жасыру керек.

- Тауарлар мен қызметтерді төлеуге келетін болсақ, кез келген жағдайда картамен сатып алу құны мен есептен шығару сомасын мұқият тексеріп, сақтықпен төлеу керек. Интернет-дүкендерде бұл мәселе ерекше өзектілікке ие. Күмәнді сайттарда сатып алу-тауарсыз және ақшасыз қалу қаупін жоғарылатады.

Нәтижесінде картаның иесіегер сақтық шараларын сақтаса, өз картасының сенімділігін айтарлықтай арттырады. Дегенмен, бұл жеткіліксіз. Картаны мобильді банк қызметіне қосу пайдалы болып табылады, ол жасалған әр төлемдерді, өзгерістер мен картадағы жасалған транзакциялар бойынша барлық ақпараттарды карта иесінің ұялы телефонына жібереді.

Қорытындылай келе , банк секторындағы қылмыстық белсенділік деңгейінің өсуіне қарамастан, карточкалар Қазақстанның және шет елдердің тұрғындары арасында танымал бола бастады. Төлем карточкаларын шығарған банктер төлем карточкаларындағы алаяқтықты азайту үшін олардың көлемін ұлғайту және қорғаудың жақсартылған деңгейімен ғана шығаруды жалғастыруда. Карточканы пайдаланушылар қылмыстық әрекеттің құрбаны болған адамның қателігін қайталамау үшін пластикалық карталарды қолданған кезде ұқыпты және сақ болулары керек.

Пайдаланылған әдебиеттер тізімі:

1. https://www.nwab.ru/static/single/-rus-common-materials41618_154419

2. Александр Захаров. Мошенничества с банковскимикартами 2019 //https://aferizm.ru/moshen/pp_plast_kart.htm

3. ҚР Ұлттық банкі // https://nationalbank.kz/?docid=3330&switch=russian