

Алаяқтар мен заманауи технологиялар: олардан қалай қорғануға болады?

«In business kz» ақпараттық агенттігінің материалдары бойынша

Азаматтарға өздерін және ақшаларын қаржылық алаяқтардан қорғауға көмектесетін қарапайым сақтық шаралары.

Соңғы жылдары Қазақстанда алаяқтықтың жаңа түрлері қарқынды дамып, жетілуде. Қылмыстық ниеттерін жүзеге асыру үшін алаяқтар көбінесе заманауи технологияларды қолданады.

Азаматтарға өздерін және ақшаларын қаржылық алаяқтардан қорғауға көмектесетін қарапайым сақтық шаралары. Тегін зат оңай келмейді.

ҚАУПСІЗДІКТІҢ ҚАРАПАЙЫМ ҚАҒИДАЛАРЫ



белгісіз немесе күдікті адресстерден түскен электрондық хаттарды ашпаңыз, электрондық пошта, әлеуметтік желілер немесе SMS арқылы жіберілген күмәнді дереккөзден жіберілген сілтемелерді ашпаңыз;



егер сіз онлайн-сатып алуды жиі жасасаңыз, онда интернет-сатып алу үшін бөлек карта жасаған дұрыс



онлайн - сатып алуды жасамас бұрын, сіз тұрған сайт шынымен интернет-дүкенге тиесілі екеніне және оның адресі <http://> емес, <https://> басталатынына көз жеткізіңіз;



төлем карталарыңызға SMS-хабарлама сервисін қосыңыз;



ешқашан төлем картаңыздағы 3D-Secure функциясын ешқашан өшірмеңіз;



PIN-кодтарды карточкалармен бірге сақтамаңыз, және оларды ешкімге айтпаңыз;



PIN-кодтарды карточкалармен бірге сақтамаңыз, және оларды ешкімге айтпаңыз;



Шұғыл түрде банкке хабарласыңыз, егер

- өз шоттарындағы ерекше белсенділікті байқадықсаңыз;
- шоттарыңызға қашықтан қолжетімділік болмаса;
- картаңыз қызмет көрсетуге қабылдамаса.

inbusiness.kz

Телефон қоңыраулары

Желіде алаяқтардың қазақстандықтарға ұялы телефонға қалай қоңырау шалып, өздерін банк қызметкерлеріміз дейтіні туралы көптеген оқиғалар бар. Сондай-ақ, олар банк терминологиясын қолдана отырып, сауатты және сенімді түрде сөйлейді. Мысалы, алаяқтар төлем картасында күдікті операциялар табылғанын мәлімдейді және оларды «бұғаттау» үшін жүйеге карта иесінің деректерін енгізу қажет дейді: ЖСН, картамен байланысты телефон нөмірі,

банктік карта нөмірі, ағымдағы немесе жинақ шотының нөмірі. Клиент деректемелерді көрсеткен кезде, олар клиенттің нөміріне жіберілген SMS хабарламаның кодын жазуды немесе ақша аударымын бұғаттау үшін оны телефондағы тон режимінде теруді сұрайды. Кодты алғаннан кейін алаяқтар, әдетте, клиенттің интернет-банкингіндегі телефон нөмірін өзгертеді және шоттардан ақшасын алады. Мұндай жағдайда не істеу керек? Бұндай жағдайда, қызмет көрсететін банкіне қоңырау шалып, ақпаратты нақтылаған дұрыс. Сондай-ақ, сіздің шотыңызға алаяқтық шабуыл жасау әрекеті бар екені туралы банкке өтініш жазған жөн. Банк қызметкерлерінің іс-қимыл регламенті бар, соған сәйкес банк қызметкерлері ешқашан бірінші болып, клиентті карта деректерін немесе SMS алынған деректерді талап етпейді. Осы мәселелер бойынша кез-келген байланыста тек клиентпен бастамашы болады.

Интернеттегі тұзақтар

Қаржылық алаяқтықтың бір түрі, әдетте, сатушы мен сатып алушының қарым - қатынасы бақыланбайтын, интернет-сауда алаңдарымен де байланысты. Мұнда көбінесе «жасырын» алаяқтар жұмыс істейді. Олар тауарды сатып алып, алдын ала төлем жасағысы келетіні жайында клиентті сендіреді, бірақ бұл үшін, әрине, төлем картасының деректемелері және SMS код - ақша аударымын іске қосу үшін клиенттің нөміріне жіберілген хабарлама қажет дейді. Схема біріншіге ұқсас: жалған сатып алушылар барлық ақшаны шоттардан алып, іздерін жасырады. Айтпақшы, сатушыны, тауарды тексерместен, ешқашанда алдын-ала төлем жасамаңыз. Интернет-алаяқтар бірнеше секунд ішінде сіздің шотыңызды бұзуы мүмкін, әсіресе егер сіз фишингтік сайттың «тұзағына» түссеңіз. Бұл алаяқтардың тағы бір түрі, зиянкестер фишингтік сайт деп аталатын төлем карталарының деректемелерін алу мақсатында танымал интернет-дүкеннің, банк сайтының немесе әлеуметтік желінің клонын жасайды. Олар сілтемелерді қолда бар почта адрестері базасы арқылы таратады, оның ішінде сіздің адресіңіз де болуы мүмкін. Фишингтік сайттармен қалай күресу керектігін білу үшін Сізге Интернетті, оны қалай қолдану керектігін және ақпаратты қорғау әдістері туралы аз болса да білуіңіз керек. Алаяқтардың тұзағына түспеу үшін бірнеше қағиданы есіңізде сақтаңыз: өз дербес деректеріңізді еш жерде көрсетпеңіз; сайттың ресімделуіне назар аударыңыз; адрес жазатын жолдағы сілтеменің дұрыстығын тексеріңіз; https қорғалған қосылуын пайдаланыңыз; күдікті хаттарды сүзгіден өткізіңіз; банк аккаунттарына кіру үшін ашық Wi-Fi нүктелерін қолданбаңыз. Құпия деректеріңізді ешкімге айтпаңыз: төлқұжат деректері, аударым туралы мәліметтер (әсіресе құпия аударма код туралы).

Қарапайым қауіпсіздік ережелері

Егер алаяқ сіз туралы жеткілікті ақпаратты жеткілікті білетін болса, ол сіздің атыңыздан тауарлар мен қызметтерді сатып ала алады, жаңа шоттар аша алады, ақша аударымын жүргізе алады немесе кредит алуға өтініш бере алады. Осындай жағдайларға жол бермеу үшін, келесі қарапайым қағидаларды орындаңыз:

- компьютеріңіз бен мобильді құрылғыларыңыздың қауіпсіздік функцияларын пайдаланыңыз (вирустан қорғау, күрделі құрама парольдер, оларды кезең-кезеңімен ауыстырып отыру керек, компьютерде немесе мобильді құрылғыда жеке деректерді ашық түрде сақтамаңыз);
- Интернетте жеке және банктік деректерді жарияламаңыз (форумдар, әлеуметтік желілер және т. б.);
- қаржы ұйымдарының қызметкерлері ұсынатын бейтаныс адамдардың қоңырауларына сенбеңіз, оларға өзіңіздің дербес деректеріңізді, әсіресе PIN-кодты, CVV-кодты (картаның артқы жағындағы үш таңбалы нөмір) ашпаңыз;
- белгісіз немесе күдікті адрестерден түскен электрондық хаттарды ашпаңыз, электрондық пошта, әлеуметтік желілер немесе SMS арқылы жіберілген күмәнді дереккөзден жіберілген сілтемелерді ашпаңыз;
- егер сіз онлайн-сатып алуды жиі жасасаңыз, онда интернет-сатып алу үшін бөлек карта жасаған дұрыс; онлайн - сатып алуды жасамас бұрын, сіз тұрған сайт шынымен интернет-дүкенге тиесілі екеніне және оның адресі <http://> емес, <https://> басталатынына көз жеткізіңіз;
- төлем карталарыңызға SMS-хабарлама сервисін қосыңыз; ешқашан төлем картаңыздағы 3D-Secure функциясын ешқашан өшірмеңіз;
- PIN-кодтарды карточкалармен бірге сақтамаңыз және, әрине, оларды ешкімге айтпаңыз, банктік карталарыңызды үшінші тұлғаларға (тіпті туыстарына), соның ішінде кафелер мен мейрамханаларда төлем жасау үшін бермеңіз.

Шұғыл түрде банкке хабарласыңыз, егер:

- өз шоттарындағы ерекше белсенділікті байқадықсаңыз;

- шоттарыңызға қашықтан қолжетімділік болмаса;
- картаңыз қызмет көрсетуге қабылдамаса.

Қаржы пирамидалары

Азаматтардан ақша алудың ең танымал және кең таралған тәсілі - бұл қаржы пирамидасы. Қаржылық немесе басқаша айтқанда, инвестициялық пирамида - бұл кіріс алу моделі, мұнда қаражатты жаңадан тартылған қатысушылардан (төменгі) жоғары тұрғандарға - пирамиданың «жоғарғы жағындағыларға» қаражатты қайта бөлу жүргізіледі.



ҚАРЖЫ ПИРАМИДАЛАРЫНЫҢ БАСТЫ БЕЛГІЛЕРІ:

1. Сізден кіру жарнасын төлеуіңізді сұрайды, жаңа клиенттерді әкелуді сұрайды және т. б.
2. Басқа салымшылардың салымдарынан жаңа қатысушыларға жоғары сыйақы, ақшалай қаражат төлеу туралы уәде беріледі.
3. Қаржы реттеушісінде ақша қаражатын тартуға арналған қызметті жүзеге асыру бойынша лицензиясының болмауы.
4. Ұйым нарықтық деңгейден бірнеше есе көп бұрын-соңды болмаған жоғары кіріс алуға уәде беретін белсенді жарнама болады.
5. Ұйым қызметінің нақты анықтамасы жоқ немесе қызметтің кейбір түрлерімен (инвестициялық компания, желілік маркетинг, тұтыну кооперативі және т.б.) бүркемелену

?

inbusiness.kz

Қаржы пирамидасының қарапайым схемасы: ұйымдастырушы алғашқы қатысушыларға өз қаражатынан үлкен табыс төлейді, бұл ретте, алғашқы қатысушылар аз жарна төлейді. Біраз уақыт пирамида ұйымдастырушысы

қатысушыларды жинайды мен олардың беделін анықтайды. Сыйақы жаңа қатысушылардың қаражатынан төленеді. Белгілі бір қатысушылар саны мен үлкен сома жиналған кезде ұйымдастырушы қатысушылардың барлық ақшасын алады да, жоқ боп кетеді. Мұндай схемасы бар пирамидалар көбінесе өздерін инвестициялық немесе қайырымдылық қорлары ретінде көрсетеді. Қаржы пирамидасының белгілері қандай?

Олардың негізгілерін қарастырайық:

1. Сізден кіру жарнасын төлеуіңізді сұрайды, жаңа клиенттерді әкелуді сұрайды және т. б.
2. Басқа салымшылардың салымдарынан жаңа қатысушыларға жоғары сыйақы, ақшалай қаражат төлеу туралы уәде беріледі.
3. Қаржы реттеушісінде ақша қаражатын тартуға арналған қызметті жүзеге асыру бойынша лицензиясының болмауы.
4. Ұйым нарықтық деңгейден бірнеше есе көп бұрын-соңды болмаған жоғары кіріс алуға уәде беретін белсенді жарнама болады.
5. Ұйым қызметінің нақты анықтамасы жоқ немесе қызметтің кейбір түрлерімен (инвестициялық компания, желілік маркетинг, тұтыну кооперативі және т.б.) бүркемелену .

Егер сіз өз ақшаңызды сеніп тапсырғыңыз келетін ұйымда жоғарыда аталған белгілердің кем дегенде бірнешеуі болса, сізді қаржы пирамидасына тартқалы жүрген жоқ па? Ойланғаныңыз жөн! Көріп отырғаныңыздай, желіде де, офлайнда да көптеген тұзақтар бар. Бұндай тұзаққа әр түрлі жастағы және қаржылық жағдайы әр түрлі адамдар ілінуі мүмкін. Әрине, кредит төлеуде қиындықтарға тап болған үмітсіз қарыз алушы заңды делдалдық фирмада жұмыс істейтін алаяқтарға көбірек сенеді және кредитті аз төлем төлеу арқылы құтылу үшін банкпен «келісуге» өз келісімін береді. Кейбір қазақстандықтар алаяқтарға сенеді, оларды «кредиттік құлдықтан» құтқаруға немесе кредит тарихын символдық сомамен «қайта көрсетуге» уәде береді, оларға ақшадан басқа, жеке басын куәландыратын құжаттардың, ЭЦҚ және басқа да құнды мәліметтердің деректерін береді. Картадан ақша алу немесе сізге біреудің кредитін «іліп қою» үшін сіз ұсынған деректер алаяқтарға жеткілікті.