

АЛАЯҚТЫҚ ӘРЕКЕТТЕРДІҢ АЛДЫН АЛУ ЖӨНІНДЕГІ ЖАДЫНАМА

Интернет желісі ақпарат алмасудың ең үлкен құралы бола отырып, сонымен бірге ақпараттық технологияларды қолданумен байланысты қылмыстардың қарқынды өсуін тудырады.

Интернетте сату кезінде Сатып алушының алаяқтық белгілері:

1. Сатып алушы өнімге аса қызығушылық танытпайды, сатып алуға деген ұмтылысын тез көрсетеді және төлем әдісі туралы сөйлесуге көшеді.
2. Сатып алушы сізден толық карта деректемелерін, соның ішінде тегі-аты-жөніңіздің латын тілінде жазылуын, жарамдылық мерзімі және CVC кодын атауды сұрайды. Осы деректердің көмегімен ол сіздің картаңызбен интернетте оңай төлем жасай алады.
3. Сатып алушы сізден төлем жасау үшін қажет деп ұялы телефоныңызға келген түрлі кодтарды беруіңізді сұрайды.

Интернетте сатып алу кезінде сатушының алаяқтық белгілері:

1. Мекен-жайы мен телефоны жоқ, барлық байланыстарды электрондық пошта немесе жедел хабар алмасу қосымшалары арқылы жүргізу ұсынылады.
2. Сатушының нақты аты жоқ, адам «лақап аты» артында жасырылады.
3. Сатушы жақында қызметке тіркелді, сату туралы хабарландыру оның жалғыз хабарламасы болып табылады.
4. Хабарландыру қателіктермен жарияланды, тыныс белгілерінсіз, бас әріптермен және т. б.
5. Өнімнің фотосуреті жоқ немесе Интернеттен алынған сурет қоса беріледі (мұны қайталанатын суреттерді іздеу қызметтері арқылы анықтауға болады).
6. Басқа сатушылардың аналогтарымен салыстырғанда тауардың бағасы тым төмен.
7. Сатушы толық немесе ішінара алдын-ала төлемді талап етеді (мысалы, сіз тауарды пошта арқылы алуға баратындығыңызға кепілдік ретінде).
8. Сатушы төлемді тек анонимді деректемелерге қабылдайды: электрондық әмияндар, ұялы телефонды толықтыру немесе басқа адамның (туысының, досының және т.б.) атына.

Телефон алаяқтығының құрбаны болмау үшін:

- Туыстарының атынан телефон арқылы қоңырау шалу және қиын жағдай туралы хабарлау кезінде сіз хабарласып отырған туыстарыңыз немесе жақындарыңызбен байланысқа шығып, болған оқиғаның егжей-тегжейін анықтап, бейтаныс адамдарға ақша аудармаңыз және бермеңіз;
- Есеп айырысу шоты/карта бойынша қызмет көрсету мәселелері туралы хабарлама келіп түскен банктің кез келген бөлімшесіне қоңырау шалыңыз және туындаған барлық мәселелерді шешіңіз. Сіз сондай-ақ заманауи технологияларды жақсы білетін жақындарыңызға қоңырау

шалып, келіп түскен хабарлама туралы айтып, кеңес сұрай аласыз. Есте сақтаңыз: бірде-бір банк карта иесінен телефон арқылы әрекет етуді немесе карта деректемелерін хабарлауды сұрамайды;

- Бейтаныс адамдарға өздеріңіз, жақындарыңыз, туыстарыңыз туралы, банк карталары жайлы, яғни кез-келген құпия ақпарат туралы мәлімет бермеңіз;
- Тауар немесе уәде етілген төлем (қызмет) үшін алдын-ала төлем жасамаңыз, төлемді нақты алған кезде ғана жүргізіңіз.

Интернеттегі алаяқтықтың құрбаны болмау үшін:

- Интернет-сайттың ақпаратын, шолуларын мұқият зерделеп, қызығушылық тудыратын тауардың бағасын салыстыру керек. Ақпараттың жетіспеушілігі, тауарды алудың түсініксіз жүйесі көбінесе алаяқтықтың белгілері болып табылады;
- Сатушы немесе дүкен туралы максималды ақпарат алу үшін: мекен-жайлар, телефондар, әлеуметтік желілердегі тарих, жеткізу қызметінің болуы және т. б. Заңды түрде жұмыс істейтін интернет-дүкендер немесе бөлшек саудагерлер толық ақпаратты орналастырады және «жеткізілгеннен кейін тауарға ақы төлеу» қағидаты бойынша жұмыс істейді;
- Сіз өзіңіздің пластикалық карталарыңыз туралы ақпарат бермеуіңіз керек (электрондық пошта арқылы жібермеңіз). Қылмыскерлер олардың реквизиттерін пайдаланып, әртүрлі сатып алулар жасай алады.

Ұялы және сымды байланыс желілерінде және Интернет желісіндегі алаяқтық түрлері

1. Ұялы және сымды байланыс арқылы жасалатын алаяқтықтар:

а) Ұялы және сымды телефон дауыстық ақпаратты беру құралы ретінде қолданылады, олардың түрлері: «Сіздің ұлыңыз апатқа ұшырады...», «Анам / әкем менде қиындықтар бар...», «бұл банктен және т. б...».

б) Ұялы телефон жалған ақпаратпен SMS жіберу үшін қолданылады: «Анашым, маған осы нөмірге ақша салыңыз, содан кейін мен бәрін түсіндіремін», «сіздің картаңыз бұғатталған, мәліметтер үшін тел..», «сіздің шотыңыздан ақша есептен шығарылды, тел...».

в) Ұялы телефонды және Интернет желісіндегі жарнамаңызды алаяқ сізден карта деректерін алу және картаны алаяқтың ұялы телефонына байланыстыру үшін пайдаланады:

«мен сіздің сайтыңыздағы жарнамаңызбен (сату, жалға беру туралы) маған картаңыздағы деректерді және артқы жағындағы кодты хабарлаңыз мен сізге ақша жіберемін...»;

«мен сізге сайттағы тауар үшін картаға ақша жібергім келеді, жалдау ақысын алдын ала төлегім келеді, сізде мобильді банкке карта байланған, егер жоқ болса, банкоматқа барыңыз мен сізге мобильді банкті қалай қосу керектігін нұсқаймын».

Хабарламаны алған кезде көрсетілген нөмірлерге қайта қоңырау шалудың қажеті жоқ. Алаяқтар ақшаны курьерге тапсыруды, оны картаға, ұялы телефон нөміріне аударуды талап ете алады, сізден банктік картаңыз туралы ақпарат алуға тырысады, банкоматқа баруды ұсынады және банкоматтан қандай да бір операциялар жасайды, сізге телефонға келетін кодтарды хабарлауды сұрайды.

Кіріс қоңырауды алған жағдайда, әңгімелесуші өзінің шынайылығына сенімділік берсе де, әңгімені тоқтату керек. Алаяқтар адастырудың психологиялық әдістеріне ие немесе жәбірленуші мен оның жақындары туралы ақпаратқа ие. Алаяқтықтың ұқсас жағдайлары Интернет желісінде де кездеседі, бірақ көмек туралы хабарлама туысының жалған парағынан әлеуметтік желідегі хабарлама арқылы беріледі.

Алынған ақпараттың дұрыстығына күмәнданған кезде жақын адамдарыңызға хабарлама келген адамның атынан қайта қоңырау шалып, картада немесе шартта көрсетілген телефон арқылы банкке қоңырау шалып, банктің жақын жердегі бөлімшесіне бару керек. Банк ешқашан телефон арқылы клиенттің картасы туралы мәліметтерді сұрамайды: оның нөмірі, артқы жағындағы коды, карта иесінің аты-жөні және оның қолданылу мерзімі, тіпті пин-код. Егер әңгімелесуші сізден осындай ақпаратты алуға тырысса немесе сіздің телефоныңызға Банктен келген кодтарды хабарлауды сұраса, онымен сөйлесуді тоқтатыңыз.

Қарт туыстары, көршілері, таныстары бар азаматтар оларға алаяқтықтың қандай тәсілдері бар екенін, алаяқтық сипаттағы қоңыраулар мен хабарламаларды алу кезінде өзін қалай ұстау керектігін, атап айтқанда алаяқтармен диалог жүргізбеу, әңгімені тоқтату және туыстарына қоңырау шалу керектігін түсіндіруі керек. Егер қарт адам банктік картаға зейнетақы алса, онда картадан ақша алуға көмек көрсетіңіз немесе туысқаныңызға картаны Сізге беруді ұсыныңыз. Алаяқтық қоңырау түскен кезде бұл факт туралы дереу полицияға хабарлау қажет.

Егер алаяқтық кезінде, телефон арқылы сөйлесу барысында қылмыскер банк картасы туралы ақпарат алса, онда картада көрсетілген телефонға қоңырау шалып, картаны бұғаттау қажет. Алаяқтық жасалған күні Банкке ақшалай қаражатты картаға қайтару туралы өтінішпен жүгіну қажет, өйткені егер операция жасалған күні карта иесі даулаған болса, банк ақшалай қаражатты қайтаруға міндетті.

Алаяқтықтың алдын алу үшін Интернет желісінде ұялы нөмірлер туралы мәліметтерді оларды сауалнамалық деректерге байланыстыра отырып таратпауға, әлеуметтік желілерде ұялы нөмірлерді, хабарландыруларда көрсетпеуге, ұялы телефон нөмірінің жанында аты-жөнін, тұрғылықты мекен-жайын және басқа да жеке ақпаратты көрсетпеуге кеңес береміз. Интернет желісінде «мобильді банкте» жұмыс істеу үшін пайдаланылатын банк карталары мен ұялы телефон нөмірлері байланған ұялы телефон нөмірлерін пайдаланбаңыз.

Соңғы уақытта ақысыз жарнамалық сайттарда тауарларды сататын Интернет желісінің пайдаланушыларына қатысты жасалған алаяқтықтар

таралуда. Сатушыға сатып алушыдан қоңырау түседі. Сатып алушының атын жамылған алаяқ тауарды сатып алғысы келетінін, бірақ басқа қалада тұратынын және тауарды сатушының картасына ақша аудару арқылы төлеуді ұсынатынын хабарлайды. Ол үшін сатушыдан карта нөмірін, карта иесін, картаның жарамдылық мерзімін, артқы жағындағы кодты, сондай-ақ картаға байланған ұялы нөмірді атауды сұрайды немесе әдепкі бойынша жарнамада көрсетілген нөмірді пайдаланады. Осы мәліметтерді алғаннан кейін алаяқ Интернет желісіндегі сатып алулар үшін төлем жасау үшін карта деректерін пайдаланады. Тағы бір нұсқа, сатушының телефонына банктен кодтар келіп түскенде және алаяқ оларды ақша аудару үшін хабарлауды сұрағанда, сол кезде алаяқ жәбірленушінің телефонына немесе оның телефонына «мобильді банк» қызметін қосып, картадан ақша ұрлайды. Үшінші нұсқа, «сатып алушы» рөлін атқаратын алаяқ сатушыны банкоматқа баруды және кейбір операцияларды жүргізіп, ақша алуды ұсынған кезде, көрсетілген үш жағдайда алаяқ сатушының қолма-қол ақшасын ұрлап кетеді.

г) Ұялы телефонды алаяқтар SMS хабарламаларын, хабарламаларды зиянды ақпараты бар Telegram, WhatsApp мессенджерлері арқылы жіберу үшін пайдаланады.

Осы хабарламаны алған кезде көрсетілген сілтеме бойынша өтуден және алынған сілтемелерді белсендіруден бас тартыңыз. Мүмкін болса, іздеу жүйелерінде Интернет желісінде осы сілтемелер мен ықтимал алаяқтықтар туралы мәліметтер бар-жоғын тексеріңіз. Интернет желісінің пайдаланушыларына бұл сілтеменің алаяқтық екенін хабарлаңыз. Егер сіздің құрылғыңызға зиян тигізбегеніне сенімді болсаңыз, көрсетілген хабарламаны жойыңыз.

Зиянды бағдарламаларды алаяқтар үнемі жасайды және жетілдіреді, ал телефонмен жұмыс істеу кезінде сіз өзіңіздің белсенділігіңізді қажет етпейтін және операциялық жүйенің осалдықтары арқылы мобильді құрылғыға жүктелуі мүмкін зиянды бағдарламалардың түріне тап болуыңыз мүмкін.

Мобильді құрылғыны жұқтырған жағдайда, хакердің мобильді құрылғыға кіруінің қауіптері мен салдарын анықтауды ұсынамыз.

Мобильді құрылғының инфекциясының белгілері операциялық жүйені бұғаттау, кіріс SMS хабарламаларын бұғаттау, мобильді құрылғы жасаған жасанды хабарламаларды жіберу болуы мүмкін. Ондай ұялы телефонды дереу өшіру керек. SIM-картаны оператордан қайта шығарып, алаяқтық жасалған болса, телефонды полицияның кейіннен тексеруі үшін сақтаңыз немесе ақша ұрланған болса, қызмет көрсету орталығына жіберіңіз.

Егер осы мобильді құрылғыға банктік карта, «мобильді банк», «Онлайн Банк», «Интернет – банк» сияқты банктік қызметтер байланған болса, онда банкпен шұғыл байланысып, картаны бұғаттап, шоттар бойынша қызмет көрсетуді тоқтата тұру қажет. Егер телефонның көмегімен мұны істеу мүмкін болмаса, онда сіз банктің ең жақын бөлімшесіне хабарласуыңыз керек. Егер мобильді құрылғы әлеуметтік желілердегі беттерге кіру үшін

пайдаланылса, онда басқа құрылғыдан немесе компьютерден әлеуметтік желіге кіріп, байланысқан телефон нөмірін өзгерту керек.

Вирус жұққан мобильді құрылғы сонымен қатар телефондағы контактілер арқылы зиянды ақпаратты тарату көзі болып табылады. Электрондық поштаның алдын алу үшін сіз өзіңіздің проблемаңыз туралы және сіздің атыңыздан келетін зиянды хабарламалар туралы ең көп таныстарыңызды хабардар етуіңіз керек.

Егер Сіздің телефоныңыздан немесе банктік картаңыздан ақша ұрланған болса, ұрлық жасалған күні банкке ақша қаражатын қайтаруды, шотыңызды бұғаттауды, сіздің шотыңыздан басқа шоттарға ақша қаражатын аударуға тыйым салуды, сіздің қаражатыңыз аударылған шоттарға қызмет көрсетуді тоқтата тұруды талап етіп жүгіну қажет. Банктен жауап алғаннан кейін, шот бойынша үзінді көшірмемен полицияға хабарласыңыз.

Егер сіз келесі нұсқауларды орындасаңыз, осы алаяқтық құрбандарының тағдырын болдырмауға болады:

- Банк карталарымен, «мобильді банк», «Банк-онлайн», «Интернет-банк» жүйелерімен және т. б. жұмыс істеу үшін Интернет желісінде сөйлесуге және көңіл көтеруге арналмаған жеке мобильді құрылғыны пайдалану;
- Интернет желісіндегі, хабарландырулардағы және әлеуметтік желілер беттеріндегі Байланыс телефондары ретінде банктік карталармен жұмыс істеу және банктік шотты қашықтан басқару үшін пайдаланылатын мобильді құрылғылардың нөмірлерін көрсетпеу;
- Ресми көздерден мобильді құрылғыға лицензиялық антивирустық бағдарламалық қамтамасыз етуді сатып алу және орнату;
- Картадан, шоттан ақша қаражатының барлық көлемін аударуға тыйым салу.

Интернет желісінде және Интернет желісінің көмегімен жасалатын алаяқтықтар:

- а) Интернет желісінде тауарларды алдын-ала төлеу бойынша сатудағы алаяқтық (жалпы түрлері: Iphone, цифрлық, тұрмыстық техника, киім, аяқ киім, автомобильдер, автомобиль бөлшектерін сату);
- б) Интернет-дүкеннен, мәлімделгенге сәйкес келмейтін тауарды сатушыдан алу.

Алаяқтықтың бұл түрлерінің дамуы адами факторларға байланысты, мысалы, үнемдеуге деген ұмтылыс, осындай тауарлармен жақын орналасқан дүкендердің болмауы, нарықта ұсыныстардың толық болмауы. Сатып алынатын негізгі тауарлар-сәнді тауарлар: қымбат сандық жабдықтар, автомобильдер, тондар, брендтік заттар. Бірінші қажеттіліктегі тауарларды сатып алу фактілері толығымен алынып тасталды. Ақшаны үнемдеуге деген ұмтылыс көбінесе барлық қолма - қол ақшаны жоғалтуға әкеледі, осыған байланысты бірінші және негізгі ұсыныс-заттарды нақты құнына сатып алу және 30-50% пайдасы бар ұсыныстарды іздемеу, өйткені бұл нарықтың жалпы

принциптеріне қайшы келеді, немесе жіберілген тауар жалған, ақаулы немесе сатып алушының сұраныстарын қанағаттандырмайды.

Өздерін қазақстандық деп санайтын, бірақ com .org .biz .net .info .tv .mobi домендік аймақтарында сайттары бар интернет-дүкендерден тауарлар сатып алмаңыз

Осындай интернет-дүкенге, сатушыға Интернет желісіндегі шолуларға ерекше назар аудару керек. Дүкен, сайт қашан құрылғанын тексеріңіз. Ол бір жыл немесе одан да көп уақыт бұрын құрылған ба. Егер сайт бір айдан аз уақыт болса, онда сатып алудан бас тартқан жөн. Сіз осы дүкенде кеңсенің бар-жоғын тексере аласыз, Интернет желісінде мұндай үйдің бар екеніне көз жеткізе аласыз, оны картадан, фотосуреттерден, Яндекс, Google панорамаларынан көре аласыз. Үйде дүкен белгісі бар немесе кеңсе бөлмелері бар екеніне көз жеткізіңіз. Суреттерде сіз жақын орналасқан ұйымдардың аттарын, телефондарын біле аласыз, оларға қоңырау шалып, ақпараттың дұрыстығын біле аласыз. Интернет-анықтамалықтарда Кеңсе орталығы әкімшісінің, ресепшеннің телефондарын табыңыз, мұндай дүкеннің немесе жеке кәсіпкердің осы ғимаратта бар екеніне және өз қызметін жүзеге асыратынына көз жеткізіңіз. Алынған ақпаратты дүкен қызметкерлерімен телефон арқылы сөйлесу кезінде пайдалану керек. Егер дүкен немесе сатушы телефонмен сөйлесуден бас тартса және Telegram, Skype, WhatsApp және басқалары сияқты басқа байланыс әдістерін ұсынса немесе телефон дүкенінде жоқ болса, сатып алудан бас тарту керек. Телефон арқылы сөйлесу барысында сіз сатушының, дүкеннің қаласында екеніңізді хабарлай аласыз және тауарды алып кетуді және кеңседе қолма-қол ақша төлеуді ұсыныңыз. Үзілді-кесілді бас тартқан жағдайда сатып алудан бас тарту керек.

Автокөлік, жол техникасы, құрылыс материалдары сияқты қымбат заттарды сатып алғанда, сатушының қаласына баратын жолға ақша жұмсауды және сатушы мен тауардың бар-жоғын тексеруді ұсынамыз. Немесе қалада достар тауып, Интернет желісіндегі ұсыныстың дұрыстығын тексеруді сұраңыз. Егер мұндай мүмкіндік болмаса, онда сатушының қаласында автокөлікті сатумен және сатып алумен айналысатын адвокаттың, автофирма қызметкерінің қызметтерін төлеу және оған сатушымен кездесіп, автокөлік пен құжаттарды қарауды ұсыну үшін номиналды ақы төлеу. Бұл құрылыс материалдары мен металды сатып алуға да қатысты – сатушы қаласындағы адвокаттың қызметіне хабарласыңыз. Сізге интернет арқылы жіберілген кез-келген фотосуреттер, құжаттарды және автокөлікті жалған сканерлеу алаяқтары үшін оңай.

Қазіргі уақытта интернет-дүкендердің көпшілігі 100% алдын-ала төленеді, егер сіз осы ұсыныстарды орындасаңыз, сіз сәтті сатып ала аласыз.

Егер тауарды әлеуметтік желі арқылы сатып алу қажет болса, сатушыны мұқият тексеріп, онымен телефон арқылы байланысып, тауар туралы егжей-тегжейлі сұрап, тауардың егжей-тегжейлі фотосуретін талап етіп, тауарды курьерлік қызметпен және үстеме төлеммен жіберуді ұсыну, тауарды қайтару мүмкіндігін, алып кету мүмкіндігін талқылау қажет.

Топтағы және сатушы бетіндегі пікірлерді тексеріңіз. Егер бірнеше желі қолданушылары толығымен мақтау пікірлері мен ұсыныстарын жарияласа, онда бұл пайдаланушылардың беттерін қарап шығу керек, олар «жалған» емес пе, олардың беттерінде жеке фотосуреттері бар ма, көптеген достары бар ма. Бұл ақпаратты сатушының парағынан көруге болады. Сатушының парағы белсенді болуы керек, жеке фотосуреттерді үнемі орналастырып, альбомдарды жаңартып отыруы керек, оқу және жұмыс орны туралы мәліметтер болуы керек, ал достарында «тірі» және белсенді қолданушылар болуы керек. Сіз сатушының қай жерде екенін, қай қалада екенін нақтылай аласыз, өнімді белгілі бір қаладағы достарыңызға алуды және сатушының реакциясын бағалауды ұсына аласыз. Егер сіз желіде дүкенмен сөйлесетін болсаңыз, онда Интернет желісіндегі дүкеннің веб-сайтын, заңды және нақты мекен-жайын хабарлауды талап етіңіз. Кез келген күмән туындаған жағдайда, әлеуметтік желі арқылы 100% алдын ала төленген тауарды сатып алудан бас тартыңыз.

Интернет желісінде алаяқтық оларды қаржы пирамидаларында, кооперативтерде, микроқаржы ұйымдарында, биржаларда, букмекерлік кеңселерде, электрондық валюта нарықтарында көбейту үшін пайдаланушылардың қаражатын тарта отырып кеңінен таралуда. Құқық қорғау органдары мұндай ұйымдармен және осындай қызметтерді ұсынатын адамдармен ешқандай қарым - қатынас жасамауға кеңес береді, өйткені көптеген компаниялар мен осы компаниялардың интернет-сайттары шетелде, ұйымдар басқа мемлекеттердің заңдары бойынша жұмыс істейді немесе бастапқыда алаяқтық болып табылады және осы жобаларға жұмсалған ақшаны қайтару мүмкін емес.

в) «Жалған» сайттар, сондай-ақ фишингтік сайттар.

Алаяқтықтың бұл түрі жәбірленуші сайтты таныс деп санайды және ондағы тауарды, қызметті сатып алады немесе өзінің банктік картасының мәліметтерін көрсетеді деп болжайды.

Жалғыз ұсыныс зейінді көрсету болуы мүмкін. Сайттың мекенжай жолағына, сайттың атауына, мекенжай жолағында қандай да бір қосымша таңбалар немесе атаулар бар-жоғына, сайт «kz» домендік аймағында орналасқанына назар аудару қажет. Мекенжай жолағынан сайт атауын көшіріп, іздеу жүйесінде тексеріңіз. Атауында таныс сөздері бар, бірақ .com .org .biz .net .Info .tv. mobi және қазақстандық интернет кеңістігімен байланысты емес басқа да домендік аймақтарда орналасқан сайттарға сенбеу керек.

Сіз өзіңіздің банктік картаңыз туралы деректерді қалдыратын сайт бөлімдерін бірнеше рет тексеріңіз, сайттың құрылған күні бойынша, сайтта көрсетілген телефондар бойынша, Интернет желісіндегі шолулар бойынша, Интернет желісінің әртүрлі блок парақтарында сайттың бар-жоғын нақтылауыңыз керек. Есіңізде болсын, алаяққа картаның артқы жағындағы карта нөмірі мен коды жеткілікті (CVV интернет желісіндегі қызметтерді

сатып алу және төлеу үшін төрт саннан тұратын код). Басқа деректер, картаның жарамдылық мерзімі, ол өзі таңдай алады, ал иесінің аты-жөні сізден немесе Интернет желісінен жеке беттеріңізден біле алады.

Егер сіз осындай сайттың құрбаны болсаңыз және оны операциядан, сатып алудан кейін байқасаңыз, картаны бұғаттаңыз және операция жасалған күні Банкке оны жою және қолма-қол ақшаны қайтару үшін хабарласыңыз.

Управление образования акимата Костанайской области - Валеева М. Б.