

Күмәнді жеткізу: алаяқтар сатып алушылар мен сатушыларды қалай алдайды

Біз тауарларға онлайн тапсырыс береміз, жарнамалық сайттар арқылы заттарды сатамыз және сәлемдемелерді еш ойланбастан аламыз. Алаяқтар әдеттегі жеткізу сценарийін жәші қолданады: олар курьерлер болып көрінеді, «қауіпсіз жеткізуге» сілтемелер жібереді, SMS-тен кодты талап етеді немесе тауарды ауыстыру үшін қайтаруды пайдаланады.

Бір мақсат - адамды тез әрекет етуге мәжбүрлеу және ақпаратты тексермеу: құпия кодты хабарлау, фишингтік сілтемеге өту, ақша аудару немесе қайтаруды дұрыс қабылдамау.

«Жеткізуді растаңыз»: кодты атауды сұраудың артында не жатыр

Бұл ең қарапайым және тиімді схемалардың бірі. Адамға жеткізу қызметінен, интернет-дүкеннен немесе маркетплейстен қоңырау шалынады немесе жазады және оның атына сәлемдеме жасалғанын хабарлайды. Оны растау, алып тастау немесе басқа уақытқа ауыстыру қажет.

Кейде алаяқтар адамның атын және басқа да негізгі ақпаратты алдын ала біледі. Бұл қоңырау шынымен нақты тапсырыспен байланысты деген сезімді тудырады. Содан кейін «Жеткізуді растау үшін SMS-тен кодты атаңыз» деген өтініш келеді.

Шын мәнінде, SMS-код сәлемдемені алуды емес, аккаунтқа кіруді, теңшеулерді өзгертуді немесе басқа әрекетті растай алады. Оны бөгде адамға беру арқылы адам іс жүзінде өзі жасамаған әрекетті растайды. Қаскүнемдер қол жеткізуді одан әрі алаяқтық әрекеттер үшін пайдалана алады.

Мұндай схемалар туралы 2026 жылғы шілдеде Қазақстанның Бас прокуратурасы бөлек ескертті.

Сценарий басқаша болуы мүмкін. Мысалы, «курьер» жеткізілім кешіктірілгенін, сәлемдеме қоймада екенін немесе қайта жөнелту үшін аз мөлшерде үлес қосу керектігін айтады. Төлем үшін адамға белгілі жеткізу қызметінің сайтына ұқсас бетке сілтеме жіберіледі. Бұл шын мәнінде төлем деректерін алу үшін жасалған фишингтік ресурс.

Сілтемелер ғана қолданылмайды. «Өткізіп алған жеткізілім» туралы хабарламада QR коды болуы мүмкін, ол қайта жіберуге ақы төлеуді ұсынады. Сканерлеуден кейін пайдаланушы жалған параққа өтеді, онда олардан банк картасының мәліметтерін енгізу сұратылады.

Сондықтан белгісіз хабардан QR кодты бейтаныс сілтеме сияқты мұқият қабылдау керек.

Егер сіз шынымен тапсырыс күтсеңіз, қоңырау шалушының сценарийі бойынша сөйлесуді жалғастырмаңыз. Қосымшаны немесе дүкеннің немесе жеткізу қызметінің ресми сайты өзін ашып, сол жерде ақпаратты тексеріңіз. Егер сіз ештеңеге тапсырыс бермесеңіз, «сәлемдемені» растамаңыз және ешқандай кодты атамаңыз.

«Арнайы сервис арқылы жеткізуді ресімдейміз»

Тағы бір кең таралған схема әдеттегі сату туралы хабарландырудан басталады. Сіз затты нарыққа шығарасыз және көп ұзамай қызығушылық танытқан сатып алушы пайда болады. Ол басқа қалада екенін және жеткізілім мүмкіндігін пайдалануды ұсынады. Бір қарағанда, бәрі қисынды: сатып алушы тауарға ақы төлейді, ал курьер оны сатушыдан алады.

Бірақ содан кейін сілтеме пайда болады: «Мұнда жеткізуді ресімдеңіз», «Осы сілтеме арқылы төлем алыңыз», «Ақшаны есептеу үшін карта деректерін енгізіңіз».

Парақша белгілі сауда алаңын немесе жеткізу қызметін толығымен дерлік көшіре алады. Онда сатушыдан картаның нөмірін, оның қолданылу мерзімін, артқы жағындағы кодын немесе SMS-кодын көрсетуін сұрайды.

Төлемдерді алудың орнына адам алаяқтарға төлем деректерін беріп, рұқсатсыз операцияларға тап болу қаупін төндіреді. Қаскүнемдердің сатып алушылар ретінде пайдаланатын жалған жеткізу сервистері туралы KZ-CERT де ескертті.

Кейде алаяқтар фишингтік сайтсыз жұмыс істейді. Мәмілені ресімдеу түрінде олар алдымен «ақша алғаны үшін комиссия», «сақтандыруды», «жеткізуді резервтеуді» немесе басқа да міндетті төлемді төлеуді талап етеді. Аудармадан кейін әңгімелесуші жоқ болып кетеді.

Жеткізудің өзі проблема емес екенін түсіну маңызды. Белгісіз адам мәмілені ресми алаңнан тыс жерге апарғанда, бөгде сілтеме жібергенде немесе күтпеген төлемді талап еткенде қауіп туындайды.

Егер хабарландыру сервисі кіріктірілген төлемді немесе жеткізуді көздесе, оларды пайдаланыңыз және алаңның өзінің нұсқауларын орындаңыз. Ал егер «сатып алушы» асығып, оның сілтемесі бойынша көшуді талап етсе немесе ақшаны тек комиссия төленгеннен кейін ғана алуға болады деп сендірсе, — бұл мәмілені тоқтатып, бәрін тексеруге елеулі себеп.

Жағымсыз тосынсыймен «қайтару»

Алаяқтық схема тауар сатылған кезде де туындауы мүмкін.

Қарапайым жағдайды елестетейік: сатушы тауарды сауда алаңы арқылы жіберді, сатып алушы оны алды, содан кейін қайтаруды ресімдеді. Сәлем-сауқат қайтарылады, бірақ оның ішінде әлдеқайда арзан немесе ақаулы зат бар. Егер тауарлар сыртынан ұқсас болса, ауыстыруды бірден байқауға болмайды.

Мысалы, сатушы жарамды смартфон жіберді, ал қайтарылған кезде басқа сериялық нөмірі бар ұқсас құрылғыны немесе ақаулы тауарды алды.

Ірі сауда алаңдарында дауларды шешу және мәмілеге қатысушыларды қорғау тетіктері көзделген. Бірақ, егер нақты не жіберілгені және қандай жағдайда екендігі туралы дәлелдемелерді алдын ала сақтаса, өз ұстанымын растау әлдеқайда оңай.

Сондықтан қымбат техниканы немесе басқа да бағалы заттарды сату кезінде тауардың суретін немесе бейнесін түсіріп, оның сыртқы түрін, жиынтығын және егер бар болса, сериялық нөмірін жазып алыңыз. Сәлемдемені жеткізу қызметіне жіберу алдында орау процесін алып тастау да пайдалы.

Қайтарымды алған кезде мәміленің аяқталғанын растауға асықпаңыз. Тауарды және оның жиынтығын тексеріңіз. Егер ауыстыруды, зақымдануды немесе басқа сәйкессіздіктерді байқасаңыз, оларды бірден фото немесе бейнеге жазып алыңыз және алаңның қолдау қызметіне хабарласыңыз.

Дауды сатып алушымен жеке хат алмасуға ғана аударудың қажеті жоқ. Егер мәміле маркетплейс арқылы өтсе, онда көзделген айналыс тетігін пайдаланыңыз және жағдай түпкілікті шешілгенге дейін тапсырыс туралы мәліметтерді, хат алмасуларды, жөнелту туралы құжаттарды, фотосуреттер мен бейнежазбаларды сақтаңыз.

Неге алаяқтар жеткізуді қолданады

Себебі қарапайым: жеткізу адаммен күтпеген жерден кездесуге шынайы мүмкіндік береді. «Банктен қоңырауды» адамдардың көбісі қырағылықпен қабылдайтын болса, «курьерден хабарлама» әдеттегі нәрсе сияқты қабылданады. Сонымен бірге адам расымен де тапсырысты, кері қайтаруды немесе сатылған зат үшін төлемді күтіп отыруы мүмкін. Сондықтан «сіздің сәлемдемеңіз кешіктірілді», «курьер тапсырысты бере алмады», «алғаныңызды растаңыз» деген сөз тіркестері шынайы мәміленің бөлігі ретінде жеңіл қабылданады.

Адамды сендіру үшін алаяқтар танымал компаниялардың логотиптерін пайдаланады, сайттардың ресімделуін көшіреді, паракшалардың ұқсас мекенжайларын жасайды және адамның кейбір дербес деректеріне ие болады. Бірақ сыртқы ұқсастық хабарламаның немесе сайттың түпнұсқа екенін растамайды.

Қарапайым үш қағиданы есте сақтаңыз:

- SMS-код – курьерге арналған құпиясөз емес.
- Карта деректері – сатып алушыдан төлем алу тәсілі емес.
- Ал жіберілген сілтеме немесе QR-код – сіздің алдыңызда тұрған ресми сервис екенінің дәлелі емес.

Онлайн сауда жасаған кезде қалай қорғану қажет

1. **Құпия деректерді хабарламаңыз.** SMS-кодтарды, құпиясөздерді, PIN-кодтарды және басқа да конфиденциалды мәліметтерді олар кім болса да бөтен адамдарға беруге болмайды.

2. **Тапсырысты өзіңіз тексеріңіз.** Дүкеннің, маркетплейстің немесе жеткізу қызметінің ресми қосымшасын немесе сайтың ашып, жөнелтуші мәртебесін қараңыз.

3. **Күтпеген сілтемелер мен QR-кодтар арқылы өтпеңіз.** Әсіресе олар арқылы жеткізуді растауды, ақша алуды немесе аздаған комиссия төлеуді ұсынатын болса.

4. **Мәмілені алаңнан тыс шығармаңыз.** Хабарландырулар сервисі арқылы сатқан кезде олар көзделген болса төлем жасаудың және жеткізудің кіріктірілген құралдарын пайдаланыңыз.

5. **Кездейсоқ «комиссияларды» төлеменіз.** «Сақтандыру», «резерв», «ақшаны алуды іске қосу» және бейтаныс адамның өтініші бойынша пайда болған басқа да төлемдерге қатысты адам мұқият болу қажет.

6. **Қымбат жөнелтілімдерді тіркеп отырыңыз.** Мәміле толық аяқталғанға дейін тауардың, оның жай-күйінің, жинақтамасының, сериялық нөмірінің және қаптамасының суреті мен бейнематериалдарын, сондай-ақ құжаттар мен хат алмасуды сақтап қойыңыз.

7. **Егер деректер алаяқтарға берілген болса – бірден әрекетке көшіңіз.** Ресми арна арқылы банкке хабарласып, шотты қорғау шаралар қабылдаңыз және қажет болған жағдайда құқық қорғау органдарына жүгініңіз.

Егер сәлемдемені немесе сатылған заттың ақшасын алу үшін сізден ресми сервистің аясынан тыс шығуды, SMS-кодты айтуды, белгісіз сілтеме арқылы өтуді немесе шұғыл бірдеңе үшін ақы төлеуді сұраса, кідіріңіз де өз бетіңізбен ақпаратты тексеріңіз. Бұл сізге ақшаңызды ғана емес банктік және басқа цифрлық аккаунттарға қолжетімділікті сақтауға мүмкіндік береді.