

Әлеуметтік желілердегі алаяқтық: өзіңізді қалай қорғау керек?

Әлеуметтік желілер тек қарым-қатынас жасау мен бос уақыт өткізу орны ғана емес, сондай-ақ түрлі алаяқтардың әрекеттері үшін ыңғайлы алаңға айналғанына мәлім. Жалған ұтыс ойындары, компаниялардың жалған аккаунттары, тіпті жақын адамдарыңыздан келген хабарламалар — мұның барлығы ақшаңыз бен дербес деректердің жоғалуы тәуекеліне әкелуі мүмкін.

Мұндай оқиғаларға тап болмаудың жолдары төменде талқыланады.

Алаяқтар қандай схемаларды қолданады

Брендтер мен дүкендердің жалған парақтары

Алаяқтар акциялар, лотереялар, сыйлықтар немесе шындыққа жанаспайтын жеңілдіктерге уәде беріп, белгілі компаниялардың логотиптерін, дизайнын және тіпті сайттарының көшірмесін жасап алады. Пайдаланушы ұсынысқа қызығушылық танытқан кезде, олардан сілтемеге өтіп, карта мен құжаттардың деректерін енгізуді сұрайды. Одан кейін ол ақшасынан айырылып, дербес деректері алаяқтардың қолына түседі, ал алаяқтар кредит ресімдеп, қылмыстық схемаларда пайдаланып немесе бопсалауға дейін барады.

Шынайы кейс: өткен жылдың қараша айында Шымкент қаласының полициясы 22 жастағы Тараз қаласының тұрғыны мен оның Алматы мен Шымкент қалаларынан келген екі сыбайласын ұстады. Олар шынайы маркетплейстер мен сауда алаңдарындағы фотосуреттер мен тауарлардың карталарының көшірмелерін жасап, әлеуметтік желілерде брендтік аяқ киім мен сөмкелер дүкенінің жалған аккаунтын құрған. Сатып алушылардан алаяқтар тауар мен жеткізу ақысын ақша аударымдары немесе қашықтан шоттар арқылы төлеуді сұратқан. Әрине, адамдарға тапсырыстары келген жоқ, себебі «сатушылар» оларды бұғаттап тастаған. Алайда, сатып алушылар мұнымен келіспей, полицияға шағым түсірген, алаяқтар қолға түсті.

Өзіңізді қалай қорғау қажет: дүкеннің аккаунтын тексеріңіз («қанат белгісінің» болуын, сайтқа сілтемені, байланыстарды, шынайы мекенжайды); тәуелсіз алаңдарда дүкен жөніндегі пікірлерді оқып, зерттеңіз; күдікті сілтемелерге өтпеңіз және картаңыздың деректерін енгізбеңіз; ешқашан белгісіз адамға аударым немесе карта арқылы төлемеңіз - тек ресми сайттар мен қосымшаларды пайдаланыңыз.

«Достардан» келетін хабарламалар

Бұл, алаяқтардың ең кеңінен тараған, «сүйікті» схемасы, себебі бұл жерде достары мен туыстарына қол ұшын бергісі келетін адамдардың сезімімен ойнауға болады. Ол келесі схемамен жасалады: әлеуметтік желінің мессенджерінде адамға қарызға ақша бере тұру немесе қызына, немересіне немесе жиеніне қандай да бір байқауда дауыс беру өтінішімен хабарлама келеді. Ал шын мәнісінде оның аккаунты бұзылған болып, әлеуетті құрбанға алаяқтар жазып отырады. Сіз зиянды сілтемеге өте салысымен сіздің барлық деректеріңіз бірден сіздің телефоныңызға, ноутбугыңызға, компьютеріңізге автоматты түрде орнатылатын арнайы қосымшаның немесе вирустың арқасында алаяқтардың қолына түседі.

Шынайы кейс: бұл тәсілді алаяқтар ерекше жақсы көреді, және олардың әрекеттерінен зардап шеккендердің саны шексіз. Мысалы, тек өткен жылдың өзінде ғана құқық қорғау органдары Қазақстанда әлеуметтік желілер мен мессенджерлер арқылы жасалған 4 000 астам алаяқтық оқиғаларын тіркеген.

Өзіңізді қалай қорғау қажет: егер жақын адамыңыз ақша сұраса немесе сілтеме жіберсе – оған жеке қоңырау шалып, ақпаратты нақтылаңыз; күмәнді сілтемелерге өтпеңіз, тіпті олар таныстардан және туыстарынан келген болса да; әлеуметтік желілерде және мессенджерлерде екіфакторлы аутентификация орнатыңыз.

Жалған ұтыс ойындары мен лотереялар

Әлеуметтік желілерде қомақты ұтыстар беруге уәде ететін ұтыс ойындары мен лотереяларды жарнамалайтын посттарды жиі кездестіруге болады. Әрине, мұндай аккаунтқа жазатын кез келген адам

бірден жеңімпаз болады. Бірақ бұл орайда бір түйткіл бар: сізден сыйлық үшін «комиссия» төлеуді сұрайды. Содан кейін сіз ұтысты да, жіберген ақшаңызды да көрмейсіз.

Нақты жағдай: 2024 жылдың соңында полиция Атырау облысының тұрғынын тұтқындады, ол әлеуметтік желілерде тым сенгіш азаматтарға өзінің лотерея өкілі екенін және адамдардың жүлделерді жеңіп алғанын айтты. Бірақ ұтысты алу үшін алаяқ өзіне ақша аударуды сұрады — сақтандыру үшін. Ол құрбандарды лотерея туралы жазбаларының астынан іздеді: оларға шығып, сыйлықтар туралы жазды. Жалпы шығын 140 мың теңгені құрады, бірақ іс жүзінде, әрине, мұндай жағдайлар әлдеқайда көп, тек олардың барлығы полиция мен соттарға бара бермейді.

Өзіңізді қалай қорғау қажет: адал лотереялар мен ұтыс ойындары «комиссияларды» немесе «сақтандыруды» талап етпейтінін ешқашан ұмытпаңыз; ұйымдастырушыны тексеріңіз: оның лицензиясы немесе ресми сайты бар ма, тәуелсіз алаңдардағы пікірлерді зерделеңіз; «ұтыс» үшін жеке деректер мен деректемелерді жібермеңіз.

Жалған жұмыс орындары

Бұл да әлеуметтік желілердегі алаяқтықтың танымал тәсілі. Әдетте, мұндай хабарландырулар өте тартымды көрінеді: «Онлайн жұмыс: сағатына 5 000 теңге, ештеңе істеудің қажеті жоқ». Ал мүдделі үміткерлерден алаяқтар «тіркеу» немесе «оқу» үшін ақы төлеуді сұрайды, содан кейін жоқ болып кетеді.

Нақты жағдай: осы жылдың наурыз айында қазақстандықтар WhatsApp арқылы Ozon маркетплейсіне жұмысқа орналасу туралы ұсыныстар ала бастады. Болжам бойынша, қашықтан және күніне небәрі 30-60 минут жұмыс істеу керек, ал оны орындау үшін 20 мың теңгеден 50 мың теңгеге дейін ақы төлеуге уәде берілді. Сонымен қатар, бос жұмыс орнының егжей-тегжейлі сипаттамасы да, нақты жұмыс шарттары да көрсетілмеген, бірақ Ұлыбритания коды бар нөмірден хабарламалар келген.

Әрине, мұның бәрі алаяқтардың айла-амалдары болып шықты, және осы уақытқа дейін адамдар анда-санда мессенджерлерге осындай ұсыныстар алады. Сонымен қатар, қызығушылық танытқан адамдарға агенттік жарна, картаны тексеру немесе сатушы деңгейін көтеру сылтауымен белгілі бір соманы аударуды сұрады. Бірақ нақты маркетплейс жұмысқа орналасу кезінде үміткерлерден ешқашан ақша алмайды.

Өзіңізді қалай қорғау қажет: «екі сағаттық жұмыс үшін оңай ақша» ұсынатын жұмыс орындары мен компанияларға сенбеңіз; ешқашан «тіркеу» немесе «оқу» үшін ақша аудармаңыз; жұмыс берушіні тексеріңіз: ресми сайты, байланыстары, ол туралы пікірлер.

Love scam немесе «романтикалық схемалар»

Алаяқтар жәбірленушімен әлеуметтік желілерде танысады және болашақта манипуляция жасау үшін оған мүмкіндігінше эмоционалды байланыс орнатуға тырысады. Алаяқ жәбірленушінің «дайын» екенін түсінгеннен кейін ақша сұрай бастайды — көшу, құжаттарды ресімдеу, емделу және т.б. Қаражат түскеннен кейін «сүйіктісі» барлық байланысты күр түзіп, жоғалады.

Нақты жағдай: биыл көктемде Ақмола облысының тұрғыны әлеуметтік желілерде өзін БҰҰ бітімгері ретінде көрсеткен алаяқпен танысты. Қарым-қатынас кезінде ер адам Қазақстанға келіп, үйленуге дайын екенін мәлімдеді, бірақ демалысты ресімдеу сылтауымен 550 доллар сұрады. Әйел ақша аударды, бірақ содан кейін БҰҰ өкілдері оған хабарласып, қосымша соманы талап етті — енді әуе көлігімен ұшып баруға. Осы жерде ақмолалық әйел алданғанын түсініп, полицияға жүгінді.

Өзіңізді қалай қорғау қажет: сезімдер туралы тым тез сөйлейтін адамдарға сенбеңіз — олар көбінесе абьюзер немесе алаяқ болып шығады; ешқашан «интернет серіктестеріне» ақша жібермеңіз, тіпті олар «билет» немесе «емделуге» ақша сұраса да; іздеу жүйелері арқылы сұхбаттасушының фотосуреттері мен деректерін тексеріңіз — бұл шын мәнінде көмектесуі мүмкін.

Алаяқтардың құрбаны болсаңыз не істеу керек?

1. Картаны шұғыл түрде бұғаттаңыз және банкке алаяқтар сізді алдағанын хабарлаңыз.

2. Алаяқтармен хат алмасудың скриншоттарын жасаңыз.

3. Әлеуметтік желіні техникалық қолдауға болған оқиға туралы хабарлаңыз және полицияға арыз жазыңыз.

Бүгінгі күні әлеуметтік желілерде сергек болу шынайы өмірдегідей маңызды. Күн сайын алаяқтар күрделі амалдарды ойлап табуда, бірақ егер сіз олардың схемалары мен іс-қимылын білсеңіз, өз ақшаңызды және дербес деректеріңізді сақтай аласыз.

Материал www.fingramota.kz сайтының көмегімен дайындалды.