

«Сіздің аккаунтыңызға қауіп төніп тұр»: алаяқтар пайдаланушылардың көңіл-күйін қалай пайдаланады

Бірнеше жыл бұрын интернет-алаяқтық негізінен белгісіз туыстарының атынан жазылған мұрагерлік туралы хаттармен байланысты болды. Бүгінгі таңда схемалар әлдеқайда жетіле түсті. Алаяқтар банктердің интерфейстерін көшіруді, белгілі қызметтердің сайттарын өздеріне ыңғайлап жасап алуды және ең бастысы — адамның көңіл-күйін өз пайдасына пайдалану үшін оларға қысым жасауды үйренді.

Онлайн арқылы көңіл-күйге әсер ету

Кейбір жағдайларда алаяқтар адамдарды деректердің жоғалып кетуі және аккаунттың бұғатталуы мүмкін деп қорқытады. Сонымен қатар, жеңіл ақша табу жолын көрсетемін немесе қымбат сыйлықтар аласыз деп уәде береді. Алаяқтар кейбір жағдайларда олардың жақын достары мен таныстарын алға тарту арқылы өз ойларын іске асырады.

Қазақстанның Бас прокуратурасы ескерткен бірінші схема аккаунттың, деректердің немесе тіпті смартфондағы бүкіл деректердің жоғалып кету қорқынышына негізделген. Алаяқтар iPhone иелеріне олардың iCloud толып кеткендігі туралы хабарламалар жібереді. Пайдаланушыны асықтырады: егер сіз шұғыл түрде деректерді жаңартпасаңыз, фотосуреттер мен құжаттар жоқ болып кетеді және аккаунт бұғатталады. Кейбір жағдайларда ықтимал зардап шеккендерге аккаунтсыз құрылғының өзі де мағынасын жоғалтатынын еске салады, себебі аккаунт сол құрылғыға тіркелген деп келтіреді.

Жәбірленуші сілтеме бойынша өтіп, жалған Apple ID немесе электрондық пошта сайтына кіріп, алаяқтарға логин, құпиясөз және кейде банктік деректерді өзі жібереді. Осыған ұқсас шабуылдар Google Drive, Mail.ru және Яндекс Диск атынан таралуда.

Қазіргі заманғы схемалардың ерекшелігі — олар ешқашан тек технологияға негізделмейді. iCloud жағдайында алаяқтар жеке деректердің жоғалып кету жағдайынан қорқады. Көптеген адамдар бұлт сервисінде барлық цифрлық өмірді сақтайды: балалардың фотосуреттері, жұмыс құжаттары, хат-хабарлар, байланыстар.

Бірақ қорқыныш бұл жалғыз құрал болып табылмайды.

«Құттықтаймыз! Сіз iPhone ұтып алдыңыз»

Егер iCloud арқылы жасалған схема мазасыздық тудырса, онда тағы бір көңіл-күйге әсер ету жұмыс істейді, адамға WhatsApp, Telegram, SMS немесе поштаға: «Құттықтаймыз! Сіз iPhone / 1 000 000 теңге / автомобиль ұтысының жеңімпазы болдыңыз» деген сияқты хабарлама келеді, бұл өз кезегінде адамның ашкөздігі мен қызығушылығын тудырады.

Кейде алаяқтар танымал брендтердің, банктердің немесе маркетплейстердің аттарын жамылады. Әсіресе, адамдар сенуге дағдыланған ірі экожүйелер. Мысалы, Қазақстанда еліміздің бес жетекші банкінің және басқа да танымал сервистердің атынан берілетін жалған «ұтыс ойындары» тіркелген, мысалы, тауарларды жеткізу мен сатып алу.

Бұдан әрі сценарий бірдей дамиды: пайдаланушыдан сілтеме бойынша өтуді сұрайды; ЖСН немесе карта деректерін енгізу; «жүлде алғаны үшін комиссия» төлеңіз; жеке басын SMS-кодпен растау.

Осы кезде ақша мен деректер алаяқтарда болады.

Сума әдетте аз — 500, 1000 немесе 2000 теңге. Сондықтан көптеген адамдар операцияны қауіпті деп санамайды. Бірақ деректерді енгізгеннен кейін алаяқтар картаға қол жеткізе алады немесе ақшаны қайта есептен шығара бастайды.

Кейде схема қиындай түседі. Пайдаланушыға «жеңімпаздар кестесі», «бағы жанғандардың» пікірлері мен қалған жүлделердің есебі берілген жасанды сайт көрсетеді. Мұның бәрі болып жатқан нәрселердің шынайы көрінісін бейнелейді.

Мұндай схемалардың қарама-қайшылығы мынада: адам көбінесе болып жатқан нәрсенің қисынсыз екенін түсінеді, бірақ «сыйлық» алуға деген ниеті оны дұрыс ойынан тайдырып жібереді. Міне, сондықтан алаяқтық ұтыс ойындары интернеттің ең ұзақ қолданылатын схемаларының бірі болып қалып отыр.

«Туысыма дауыс беріңізші»

WhatsApp пен Telegram арқылы жаппай таратылатын тағы бір схема мүлдем қауіпсіз болып көрінеді.

Хабар таныс адамнан келген сияқты болады. Онда «Сәлем! Өтінемін, туысыма дауыс беріңізші. Ол байқауға қатысып жатыр еді, жеңісек жетуіне аз ғана қалды» деген мәтін көрсетіледі.

Хабарға қоса «дауыс беру» сілтемесі болады. Сайт ресми сайт тәрізді көрінеді: балалардың фотосуреттері, дауыстар есебі, байқау логотиптері. Бірақ дауыс беру үшін пайдаланушыға телефон нөмірі мен SMS арқылы келген кодты енгізу ұсынылады.

Іс жүзінде бұл — WhatsApp немесе Telegram akkaунтына кіру коды. Оны бергеннен кейін алаяқтар өз құрбанының мессенджерін толық бақылай алады.

Әрі қарай схема вирус тәрізді тарала бастайды: akkaунт иесінің атынан оның достарына жаңа сілтемелер жіберіледі; таныстарынан шұғыл түрде қарыз сұрайды; алаяқтар хат-хабарлар мен байланысатын адамдарға қолжетімділік алады.

Қазақстанда мұндай жағдайлар әлеуметтік желілерде көп рет талқыланды: адамдар бір рет «дауыс бергеннен» кейін бірнеше минут ішінде қалай мессенджерге кіре алмай қалғандарын айтқан.

Барынша көп ақпарат алғаннан кейін алаяқтар хабарларды жаппай таратып қана қоймай, ұзақ уақыт бойы «құрбанын өңдеу» арқылы жеке-жеке хабар жібере алады.

Мысалы, бір танымал коллекционердің шотын бұзғаннан кейін алаяқтар оның таныстарына ерекше экспонаттарды сатып алу үшін белгілі бір сома қарыз сұрап жазған. Оның немен айналысатыны жөнінде «хабардар» адамдар оның расында сирек кездесетін дүниеге қол жеткізуіне көмектесіп жатырмыз деп ойлап, бірнеше адам ақша жіберген. Олар аударым жасауға ұсынылған банк картасының стандартқа сай емес екеніне де мән бермеген.

Сондықтан мұндай шабуылдар әсіресе қауіпті: адам келген хабарға сенеді, өйткені ол бейтаныс адамнан емес, нақты өзі білетін адамнан келеді.

«Сізге сәлемдеме келді»

Соңғы айларда жиі қолданылып жүрген танымал схема жеткізу қызметімен байланысты. «Сіздің сәлемдемеңіз кешіктірілді», «Жеткізу мекенжайын растаңыз», «Кедендік алымды төлеңіз» деген хабар келеді. Әсіресе алаяқтар танымал маркетплейстар мен курьерлік қызметтердің аттарын жиі пайдаланады. Онлайн сатып алу дамып тұрған уақытта мұндай хабарлар шын сияқты көрінеді, сөйтіп көп адамдар жеткізілімді күтеді.

Сілтемені басқаннан кейін пайдаланушыдан: авторизациядан өтуді; банк деректерін көрсетуді; шағын «комиссия» төлеуді сұрайды.

Кейбір жағдайларда сілтеме зиянды қосымшаны орнату бетіне апарады, ол SMS және банктік хабарламаларға қол жеткізеді.

«Мына фотодағы сіз бе?»

Мессенджерлерде қайтадан танымал болып келе жатқан ескі схема. Пайдаланушыға «Фотодағы сен бе?» немесе «Сен туралы не жазғанын көр» деген хабар келеді. Ішінде — сілтеме немесе файл. Ашылғаннан

кейін құрылғы зиянды БҚ жұқтыруы мүмкін, алаяқтар аккаунттарға кіре алады немесе байланыстағы адамдар арқылы автоматты түрде тарату басталады. Кейде сілтеме Telegram немесе Instagram фишингтік кіру бетіне апарлады.

Басты міндет — қатты эмоциялық реакция тудыру: қызығушылық, алаңдаушылық немесе қорқыныш.

Адамдар неліктен ұрына береді

Көп адамдар: «Мен мұндайға тап болмаймын» деген сенімде болады. Бірақ қазіргі заманғы алаяқтық схемалар техникалық дайындығы жоқ пайдаланушыларға емес, қарапайым адамдарға арналған.

Сондықтан да киберқауіпсіздік жөніндегі мамандар мынаны үнемі қайталап отырады: бүгінгі күннің басты қорғанысы — антивирус емес, банктің немесе қосымшаның қауіпсіздік жүйесі емес, тоқтап, ақпаратты қайта тексеру әдеті.

Осындай схемалардан өзіңізді қалай қорғауға болады

- 1) Хабарлардағы сілтемелер бойынша өтпеңіз. Хат немесе SMS ресми болып көрінсе де.
- 2) Ақпаратты тек ресми қосымшалар мен сайттар арқылы тексеріңіз. iCloud немесе банк аккаунтын тексергіңіз келсе, онда ол жерге өзіңіз кіріңіз.
- 3) SMS кодтарын ешкімге айтпаңыз. Тіпті достарыңыз бен туыстарыңызға да.
- 4) «Тым жақсы» ұтыстарға сенбеңіз. Егер сіз ұтысқа қатыспасаңыз, сіз ештеңе ұтып алмадыңыз.
- 5) Таныстарыңыздың өтініштерін әрдайым қайта тексеріңіз. Дұрысы адамға тікелей қоңырау шалу керек.
- 6) Екі факторлы аутентификацияны қосыңыз. Бұл аккаунттарды бұзу қаупін айтарлықтай төмендетеді.

Егер аккаунт ұрланған болса, бірден әрекет етіңіз. Құпия сөзді ауыстырыңыз, белсенді сессияларды аяқтаңыз және бұзу әрекеттері туралы ескертіңіз.

Бүгінде алаяқтар құрылғыларды ғана емес, адамдардың эмоцияларын да бұзады. Цифрлық схемалар неғұрлым сенімді болса, хабарларға автоматты түрде жауап бермеу әдетін сақтау соғұрлым маңызды — тіпті олар шұғыл, пайдалы немесе өте «адами» болып көрінсе де.

Материал www.fingramota.kz сайтының көмегімен дайындалды.