Дербес деректеріңіз жария болған жағдайда не істеу керек: қорғану амалдары

Дербес деректердің жария болуы – бұл абстрактілі қауіп емес, күнделікті өмірде кездесетін проблема. Мәселен, тек өткен жылдың өзінде ғана жеке ақпараттарды: ЖСН, мекенжайлар, телефон нөмірлерін және басқа да деректерді қамтитын 16 миллионнан астам жазба ашық қолжетімді болды.

Сіздің деректеріңіз басқалардың қолына түсу ықтималдығын қалай білуге болатынын, олар жария болғаннан кейінгі алғашқы сағаттарда не істеу керек және болашақта қандай дағдылар мұндай тәуекелді азайтуға көмектесетінін қарастырамыз.

Дербес деректер деген не

Дербес деректер - адамның жеке басын анықтауға болатын кез келген ақпарат. Олар жалпыға қолжетімді және шектеулі сипаттағы болып бөлінеді. Біріншісіне конфиденциалдылық талаптары қолданылмайтын, яғни адамның өзі әлеуметтік желілерде көрсеткен немесе мекенжай базаларында, ашық интернет-көздерде және БАҚ-та орналастырылған деректер жатады.

Қолжетімділігі шектеулі деректерге тегі, аты, әкесінің аты, туған күні мен жылы, ұлты, тұратын немесе тіркелген мекенжайы, ЖСН, жеке куәлігінің деректері және басқа да мәліметтер жатады. Қолжетімділігі шектеулі деректер «Дербес деректер және оларды қорғау туралы» заңмен қорғалады және көп жағдайда осы деректерді қолға түсіру алаяқтар мен жосықсыз компаниялардың мақсатына айналады, олар жария болған ақпарат арқылы өз қызметтерін алдыруға тырысады. Деректердің жария болуы әрдайым адамның алаяқтардың құрбаны болады дегенді білдірмейді, дегенмен де тәуекелдер сақталады. Сол үшін оны танып, өзіңді қалай қорғауды білу керек.

Деректердің жария болуының басты белгілері

1. Сіз ешқашан деректеріңізді бермеген компаниялардан немесе сервистерден түсетін спам-қоңыраулар, хабарламалар және электрондық хаттар.

2. Сіз ешбір жерде тіркелмеген және қандай да бір қызметке тапсырыс бермеген болсаңыз да тіркелуді растау және SMS-хабарламалар.

3. Өздерін танысыңмын немесе әріптесіңмін деп таныстыратын адамдардың бейтаныс нөмірлерінен қоңыраулар. Көбінесе, сіз оларға сену үшін олар сіздің жеке ақпаратыңызды пайдаланады. Соңғы уақытта технологияның күрт дамуына байланысты тіпті сіздің дауысыңызды да қолдан жасауға болады, сондықтан сақ болыңыз.

4. Банктердің немесе мемлекеттік органдардың қызметкерлеріміз деп таныстыратындардан жиі қоңырау шалу - айына бір рет қоңырау шалу қалыпты жағдай, алайда сізге қысқа мерзімде бірнеше рет шықса, бұл сіздің деректеріңіз үшінші тұлғаларға мәлім болғанның белгісі.

5. Аккаунттардағы күдікті әрекеттер туралы хабарламалар – кодтарды сұрау, поштаға немесе әлеуметтік желілерге кіру әрекеттері, сондай-ақ жаңа құрылғылардан немесе шет елдерден кіру әрекеті.

Бірінші қадам: нақты қандай деректердің ұрланғанын анықтаңыз

Өкінішке қарай, мұны анықтау мүмкін бола бермейді — банктер, компаниялар немесе дерекқорлардың иелері үшінші тараптарда қандай мәліметтер болғанын айта бермейді. Алайда, егер сіз деректердің қолды болғанын жаңалықтардан білсеңіз немесе қандай деректердің ұрланғаны нақтыланбай хабарлама алсаңыз, шара қолданғаныңыз жөн. Әдетте, мұндай жағдайларда қаскүнемдерге электрондық және пошта мекенжайлары, құпиясөздер, атаулар, телефон нөмірлері және банктік карта деректері қолжетімді болады.

Екінші қадам: қолды болған деректерді өзгертіңіз

Әрине, тұрғылықты жеріңізді өзгертудің қажеті жоқ, бірақ әлеуметтік желілердегі, үнемі пайдаланатын сайттардағы (мысалы, мемлекеттік қызметтерді алуға арналған немесе маркетплейстердегі) есептік жазбаларды өзгертіп, қорғай аласыз. Егер сіз бұрын барлық жерде бір құпиясөзді қолдануды әдетке айналдырған болсаңыз, енді әр сервис үшін бөлек жасаңыз. Мысалы, мессенджерлерде сұрату бойынша пин-код теру функциясын, ал банктердің қосымшаларында биометрияны енгізуге болады, бұл сізді қосымша қорғайды.

Үшінші қадам: екі факторлы аутентификациялауды орнатыңыз

Бұл шараны елемей қоймаңыз – бұл деректеріңізді, ақшаңызды және жүйкеңізді сақтауы мүмкін. Мүмкіндігінше екі факторлы аутентификациялауды қосыңыз. Растаудың ыңғайлы әдісін таңдауға болады: аутентификатор қосымшасынан, телефон нөмірі арқылы, электрондық пошта арқылы немесе хабарламамен алынған код. Нәтижесінде, сіздің құпиясөздеріңіз қаскүнемдерге қолды болса да, олар аккаунттарға кіре алмайды.

Төртінші қадам: барлық есептік жазбаларыңызды үнемі тексеріп отырыңыз

Деректердің қолды болғаны белгілі болғаннан кейінгі алғашқы күндерде барлық маңызды қызметтер мен қосымшалардағы аккаунттарыңызды үнемі тексеріп отырыңыз. Болашақта да бақылауды тоқтатпаңыз: күдікті кіру әрекеттерін, белгісіз құрылғыларды және әдеттен тыс әрекеттерді қадағалаңыз. Бұдан басқа, құпиясөздерді, PIN-кодтарды, бағдарламалық қамтылымды және вирусқа қарсы бағдарламаларды үш-алты айда бір рет жаңартып отырыңыз.

Бесінші қадам: жағдайды өзіңіздің банкіңізбен талқылаңыз

Қаскүнемдер сіздің тек электрондық поштаңызға қол жеткізген болса да, мұның өзі сіздің шоттарыңызға қол жеткізуге әрекет жасау үшін жеткілікті. Пошта жиі жағдайда телефон нөмірімен байланысты, ал ол өз кезегінде интернет-банкингте пайдаланылады, мұндай жағдайда сіздің қаражатыңызға көбірек қауіп төнеді. Бұған жол бермеу үшін барлық алдыңғы шараларды қолға алу, сондай-ақ банк пен оның қауіпсіздік қызметімен хабарласу маңызды: сіздің деректеріңіздің қорғалуы олар үшін де қажет, өйткені олардың беделі осыған байланысты.

Өзіңіздің дербес деректеріңізді тағы қалай қорғауға болады?

1. Бейтаныс адамдар жіберген хаттарды ашпаңыз және күдікті сілтемелерге өтпеңіз – бұл көптеген проблемалардың алдын алуға көмектеседі.

2. Өз құрылғыларыңыздағы бағдарламалық қамтылымды тұрақты түрде жаңартып отырыңыз: жаңартулар осалдықтарды жояды және киберқауіптерден қорғауды күшейтеді.

3. Сенімді құпиясөздер мен екі факторлы аутентификацияны пайдаланыңыз – бұл цифрлық қауіпсіздіктің негізгі элементтерінің бірі. Мүмкін болатын жерлердің барлығында 2FA іске қосыңыз, ал құпиясөздеріңіз ұзақ, күрделі болсын және туған күніңіз сияқты жеке ақпаратпен байланысты болмасын.

4. Үйдегі Wi-Fi-ды қорғаңыз және ашық желілерден аулақ болыңыз: жеткілікті қорғалмаған байланыс қаскүнемдердің қол жеткізуіне көмектесуі мүмкін. Сондай-ақ, қоғамдық орындарда ашық желілер арқылы деректердің қолды болу қаупі бар.

5. Ескі қатты дискілерді дұрыс кәдеге жаратыңыз: құрылғыларда көптеген маңызды ақпарат сақталады, ал қарапайым форматтау оның толық жойылғанына кепілдік бермейді, сондықтан кәдеге жаратудың алдында тасымалдағыштарды іс жүзінде жойған дұрыс.

6. Пайдаланбайтын уақытта Bluetooth-ді өшіріңіз: қосылып тұрған байланыс құрылғыны анықтауды жеңілдетеді және рұқсатсыз қол жеткізу қаупін арттыруы мүмкін.

7. Деректерді шифрлаңыз: бұл бір қарағанда қиын болып көрінуі мүмкін, бірақ заманауи құралдар процесті қолжетімді етеді. Мысалы, macOS-та тұтастай дискіні шифрлауға мүмкіндік беретін кіріктірілген FileVault мүмкіндігі көзделген.

Өзіңізді, өз деректеріңізді сақтаңыз және қаржылық сауаттылығыңызды арттырыңыз!

Материал www.fingramota.kz сайтының көмегімен дайындалды.