

Доксинг шабуылдауда: өзіңді және өзіңнің дербес деректеріңді қалай қорғау керек

Қазақстанда цифрлық орта белсенді дамуда: онлайн-сервистер, мемлекеттік көрсетілетін қызметтер және мобильді қосымшалар саны күннен күнге артуда. Алайда, солармен қатар доксинг — адамның келісімінсіз жеке деректерді мақсатты түрде жинау, жариялау немесе тарату жағдайларының саны да өсуде.

Өзіңізді және жақындарыңызды доксинг-шабуылдарынан қалай қорғауға болатынын қарастырайық.

Қаскүнемдер жеке деректерге қалай қол жеткізе алады

Өкінішке орай, заман ағысына қарай біз әлеуметтік желілерде, маркетплейстерде, қосымшаларда тіркелуге мәжбүрміз, оны біздің деректерімізді қолға түсіру үшін осы салада азды-көпті білімі бар алаяқтарға оңайға соғуда. Олардың мұны қалай жүзеге асыратыны жөнінде әрі қарай айтып береміз.

1. Іздеу жүйелері — олардың көмегімен ескі жазбаларды, түсініктемелерді, форумдардағы еске алуларды табуға болады, ал жетілдірілген мүмкіндіктер нақты сайттар немесе файлдардың түрлері бойынша іздеуге мүмкіндік береді. Адамдардың әртүрлі платформаларда бірдей лақап атты пайдалану әдеті қосымша осалдық тудырады: бұл пайдаланушы туралы деректерді бірден бірнеше қоғамдық ресурстардан жинауды жеңілдетеді.
 2. Әлеуметтік желілер — ашық профиль іс жүзінде аты-жөні, жұмыс орны, қаласы, фотосуреттері және қарым-қатынас ортасымен дайын файлға айналады. Тіпті парақша жабық болса да, доксер ақпаратты басқа адамдардың жазбаларының астындағы түсініктемелер, қауымдастықтарға қатысу, достарының жарияланымдары арқылы жинай алады. Көп жағдайда олар қосымша деректерге қол жеткізу үшін рекрутердің немесе компания қызметкерінің атын жамылып достарға қосылады.
 3. Әлеуметтік инженерия — қаскүнемдер жеке деректерді адамның өзінен тікелей алуға қарманып, банкирдің, дәрігердің немесе ұйым қызметкерінің атынан жазуы мүмкін. Көптеген пайдаланушылар өздерін алдап тұрғанын түсінбей және ақпаратты өздері береді.
 4. Жұмыстағы қарым-қатынастар — егер басшы сайтта немесе әлеуметтік желілерде қызметкерлердің тізімін фотосуреттерімен бірге орналастырса, оны доксерлер қуана пайдаланады. Тіпті, тек кәсіптік мәлімет болып көрінетін болмашы мәліметтер бойынша адамның тұрғылықты жерін анықтауға, содан кейін әлеуметтік желілерде адамның профилін табуға болады. Коммерциялық қызмет те өз ізін қалдырады — көптеген елдерде компания құрылтайшыларының деректері ашық түрде қол жетімді.
 5. Қара нарық — даркнетте мемлекеттік органдар мен компаниялардың жария болап кеткен деректері сатылады, онда сіз төлқұжат сканерлерінен бастап банктік қосымшаларға дейін бәрін таба аласыз. Мұндай ақпарат салыстырмалы түрде қымбат болмайды, олардың болуы доксингті жеңілдетеді.
- Деректер брокерлері қылмыскерлердің құрығына түсіп қалғандарын өздері де түсінбеулері мүмкін, себебі мұндай компаниялар жеке ақпаратты көптеген дереккөздерден заңды түрде жинайды және бір жүйеге келтіріп, бизнеске сатады. Бұл деректер бөгде адамдарға арналмағанымен, олар көп жағдайда алаяқтардың қолына түсіп жатады және адам туралы мәліметтер жинауды айтарлықтай жеңілдетеді.

Егер сіздің деректеріңіз жария етілген болса не істеу керек?

Доксинг фактілерін жинақтап тіркеп жүріңіз: электрондық хаттарды, дауыстық хабарламаларды, SMS-ті жинаңыз, әлеуметтік желілерде жазбалардың немесе түсініктемелердің скриншоттарын жасаңыз. Бұл полицияға, сотқа дейінгі шағымға және т.б. жүгіну үшін қажет болуы мүмкін.

Контентті жоюды талап етіңіз: егер адам немесе ұйым сіздің жеке деректеріңізді таратқан болса, олар көбінесе жалған немесе жаңылыстыратын ақпаратпен бірге жүреді. Сіз материалды жоюды немесе түзетуді талап ететін деректер жарияланған платформаларға немесе сайттарға тікелей жүгіне аласыз.

Доксинг туралы міндетті түрде құқық қорғау органдарына хабарлаңыз, әсіресе егер ол бопсалаумен немесе қоқан-лоққы жасаумен бірге жүрсе.

Заңгермен кеңесіңіз: ол перспективалар мен ықтимал тәуекелдерді бағалауға көмектеседі, сондай-ақ Қазақстан заңнамасы тұрғысынан өзіңізді қалай қорғауға болатынын айтады.

Жеке өміріңізді қорғаңыз: барлық жерде — әлеуметтік желілерде, жұмыс аккаунттары мен сайттарда, маркетплейстерде және т.б. жеке ақпаратты барынша азайтыңыз.

Қазақстанның доксинг туралы заңнамасында не жазылған

Әрине, егер сіз доксингке тап болсаңыз, дереу полицияға және заңгерлерге хабарласқаныңыз жөн, дегенмен Қазақстанның заңдары бұл қылмыс туралы не айтатынын және қаскүнемдерді не күтетінін қысқаша айтып берейік.

ҚР Конституциясының 18-бабы әрбір қазақстандықтың жеке өміріне қол сұғылмауына, өзінің және отбасының құпиясы болуына, ар-намысы мен абыройлы атының қорғалуына, жеке салымдары мен жинаған қаражатының, жазысқан хаттарының, телефон арқылы сөйлескен сөздерінің, почта, телеграф арқылы және басқа жолдармен алысқан хабарларының құпиялылығы сақталуына кепілдік береді. Осылайша, доксинг Конституцияны тікелей бұзу болып табылады.

Әрі қарай, егер доксер бопсалаумен айналысса, онда бұл Қылмыстық кодекстің 194-бабы, ол қылмыскерге төрт жылға дейін шектеу немесе бас бостандығынан айыруға қауіп төндіреді. Ауырлататын жағдайларда мерзім 15 жылға дейін ұзартылуы мүмкін.

Қылмыстық кодекстің 147-бабы – «Жеке өмірге қол сұғылмаушылықты және Қазақстан Республикасының дербес деректер және оларды қорғау туралы заңнамасын бұзу» туралы да ұмытпау керек. Адамның жеке немесе отбасы құпиясын құрайтын, жеке өмірі туралы мәліметтерді оның келісімінсіз заңсыз жинау үш жылға дейінгі мерзімге бас бостандығын шектеуге не сол мерзімге бас бостандығынан айыруға жазаланады.

Егер қылмыскер адамның жеке өмірі туралы мәліметтерді оның келісімінсіз таратса немесе өз әрекеттерімен жәбірленушінің құқықтары мен заңды мүдделеріне елеулі зиян келтірсе, онда ол үш жылдан алты жылға дейін бас бостандығынан айырылуы мүмкін. Егер ол интернетті қолдана отырып таратылса, онда жаза жеті жылға дейін артуы мүмкін.

Өзіңізді қалай қорғауға болады

1. Өзіңіздің цифрлық ізіңізді барынша жасырын ұстаңыз: әлеуметтік желілеріңізді тексеріңіз, ескі жазбаларды жойыңыз, телефонды, мекенжайды, оқу орнын, жұмыс орнын, балаларыңыздың деректерін ашық қолжетімділіктен алып тастаңыз.
2. Әртүрлі құпиясөздер қолданыңыз: бір құпия сөзбен сіз барлық аккаунттардағы деректерді жоғалту немесе салдарынан зардап шегу қаупі бар. Сізге Bitwarden, 1Password, Google Password Manager сияқты құпиясөз менеджерлері көмектесе алады.
3. Екіфакторлық бірдейлендіруді қосыңыз: мүмкін болған жердің барлығында — WhatsApp, Instagram, Telegram, Google, eGov, Kaspi.
4. Профильдің басқаларға көрінуін шектеңіз: достарыңыздың тізімін, фотоға, геолокацияға, туған күнге, белсенділікке белгілерді жауып қойыңыз. Әлеуметтік желілеріңізді мүмкіндігінше жеке етіңіз.
5. Барлық жерде бірдей лақап ат қолданбаңыз: бірдей лақап ат сізге ондаған сайттардан досыңа жинауға мүмкіндік береді. Әр түрлі платформалар үшін әр түрлі нұсқалар болған дұрыс.
6. Мессенджерлерде бейтаныс адамдарға ешқашан құжаттарыңызды жібермеңіз: жеке куәлікті, ЖСН, ЭЦҚ, банк деректемелерін, билеттерді, анықтамаларды жібермеңіз — бұл доксингке және кредиттерді ресімдеуге тікелей жол.

7. Өз құрылғыларыңызды қолжетімділікке тексеріңіз: ескі қолданбаларды, камераға/микрофонға рұқсаттарды, байланыс деректеріне, галереяға, құжаттарға қолжетімділікті жойыңыз.

8. Ашық дереккөздерін тазалаңыз: хабарландыру қызметтерінен, ескі форумдардан, профильдік сайттардан деректеріңізді жойыңыз. Қосымша қауіпсіздік үшін іздеу жүйелерінде аты, телефон нөмірі және фотосуреті бойынша өзіңізді тексеріңіз.

9. Файлдар мен сілтемелерге сақ болыңыз: АРК файлдарын жүктемеңіз, «жұмыс бойынша», «мектептен», «банктен» деген бейтаныс сілтемелерді ашпаңыз. Әлеуметтік инженерия — доксерлердің негізгі құралы.

10. Байланыс деректерін бөліп қойыңыз, «қорғаныс» телефон нөмірін пайдаланыңыз: әлеуметтік желілер, сайттарға тіркелу, сатып алу және жеткізу қызметтері үшін жеке нөмір өте қолайлы болады. Негізгі нөмір тек жақын адамдарға белгілі болуы — бұл доксинг, спам, қоқан-лоққы және хакерлік қаупін азайтады.

Өзіңізді, жеке деректеріңізді қорғаңыз және қаржылық сауаттылықты арттырыңыз!

Материал www.fingramota.kz сайтының көмегімен дайындалды.