Шта је доксинг и како се заштитити?

Са све већом популарношћу друштвених мрежа и самог интернета, веће су и могућности за злоупотребу, па и вршњачко насиље. Шта је доксинг, може ли се избећи и како се заштитити?

Најкраће речено, доксинг представља радњу или процес тражења и објављивања приватних или идентификационих информација о одређеној особи на интернету, обично са малициозном намером. Може имати различите мотиве, укључујући освету, забаву, крађу идентитета или чак ширење мржње. У питању је облик онлајн узнемиравања који значи јавно откривање нечијег правог имена, адресе, школе, посла или других података за идентификацију без пристанка жртве. Циљ доксинга је понижавање, малтретирање, узнемиравање или на други начин наношење штете жртви. Место извођења доксинга најчешће су управо друштвене мреже и интернет: форуми, четови и онлајн игрице.

Доксери често користе информације које лако могу пронаћи на интернету, као што су јавни профили на друштвеним мрежама, постови на форумима, или чак јавно доступни телефонски именици. На пример, уколико неко на форуму или друштвеној мрежи дели своје име и град у којем живи, доксери могу користити ту информацију како би пронашли додатне податке као што су адреса и број телефона.

Зашто се доксинг јавља?

Освета је чест мотив за доксинг. На пример, ако се двоје тинејџера посвађа онлајн, једно од њих може покушати да открије и објави личне информације о другој особи како би јој нашкодило.

Зашто деца и родитељи треба да знају о доксингу?

Доксинг може имати озбиљне последице, укључујући:

Губитак приватности: доксинг може изложити личне податке детета на интернету, чиме се крши приватност и сигурност детета, као и његове породице.

Дигитално насиље или сајбербулинг (енг. cyberbullying): доксери често користе ове информације како би започели дигитално насиље и узнемиравање деце.

Физичка опасност: ако се доксер одлучи на кораке изван виртуелног света, то може довести до озбиљних физичких претњи по дете, или неко ко сазна где живи дете, може покушати да га узнемири или му науди,

Крађа идентитета: доксинг се може користити за крађу идентитета и обману других корисника на интернету.

Ширење мржње: доксери често циљају особе због њихове расне, верске, полне или сексуалне оријентације како би ширили мржњу.

Да ли је доксинг нелегалан?

Технички – не, јер доксери користе информације које су јавно доступне на интернету да стекну јасну слику и конкретне информације о жртви коју потом „нападају“ тиме што пуштају њихове податке онлајн. Оно што може попримити облике које могу имати законске последице јесу дигитално насиље, ширење мржње, крађа идентитета, због чега је важно ове претње схватити озбиљно, прикупити доказе и контактирати надлежне службе ако до тога дође.

Како се заштитити од доксинга?

Родитељи и деца могу предузети одређене кораке и савете како би се заштитили од доксинга.

Деца

• Не делите личне информације онлајн: подсетите децу да никада не деле личне информације као што су адреса, број телефона, или школски подаци на интернету.

• Правилно поставите поставке приватности: научите децу како да поставе строге поставке приватности на друштвеним мрежама и другим платформама.

• Будите опрезни с пријатељствима: деца треба да буду селективна при прихватању захтева за пријатељство и контактима на интернету.

Родитељи

• Разговарајте с децом: отворена комуникација је кључна. Разговарајте са децом о опасностима на интернету и охрабрите их да вам пријаве било какво неприкладно понашање.

• Праћење онлајн активности: активно пратите онлајн активности своје деце и упозорите их на потенцијалне ризике.

• Користите родитељске контролне апликације: постоје многе апликације и алати који вам омогућавају да пратите и ограничите интернет активности ваше деце.

• Едукација: упознајте се са појавом доксинга како бисте боље разумели опасности и знали како да их спречите.

Додатне препоруке

Свакодневно понашање на интернету може знатно утицати на ниво сигурности од доксинга. Ево неколико ствари које не треба радити како бисте додатно заштитили себе и децу од ове претње:

• Не делите личне информације јавно: избегавајте објављивање личних података као што су адреса, број телефона, датум рођења и слично на друштвеним мрежама и форумима. Што мање информација делите јавно, мање је вероватно да ће их доксери користити против вас.

• Не прихватајте непознате захтеве за пријатељство: на друштвеним мрежама, немојте прихватати непознате захтеве за пријатељство или контакте. Доксери често користе лажне профиле како би се приближили својим жртвама.

• Будите опрезни при дељењу слика и видеа: пре него што поделите слике или видео садржај, размислите о томе како би их неко могао злоупотребити. Обратите пажњу на могуће идентификационе информације у позадини слика, као што су адресе или препознатљиви локалитети.

• Избегавајте јавно расправљање о контроверзним темама: када се укључите у јавне расправе на интернету, будите опрезни са својим коментарима и не вређајте или не провоцирајте друге кориснике. Емотивне реакције у онлине дебатама могу привући непожељну пажњу.

• Не кликћите на сумњиве линкове: доксинг може почети од једног јединог сумњивог линка. Никада не отварајте непознате линкове или фајлове које вам шаљу непознати корисници.

• Будите пажљиви с лозинкама: користите јаке лозинке и не користите исте лозинке на више платформи. Ово може помоћи у спречавању хакера да приступе вашим личним информацијама.

• Пазите на фишиг или пецање (енг. phishing): будите свесни фишинг напада, где вам се лажно шаљу имејл поруке или поруке које вас маме да откријете личне информације. Проверите тачност имејл адресе пре него што кликнете на линкове или делите информације.

• Користите алате за заштиту од вируса и малвера: инсталирајте и редовно ажурирајте антивирусне програме како бисте спречили злонамерни софтвер да се инсталира на вашем уређају.

• Обавестите надлежне органе о злостављању: ако постанете мета доксинга или дигиталног насиља, одмах обавестите локалну полицију и интернет сервис провајдера о инциденту.

Закључак

Доксинг представља озбиљну претњу онлајн безбедности и приватности. Деца и родитељи, као и саме школе, треба да буду обазриви и едуковани о овој појави како би се заштитили. Комуникација, стално информисање и постављање строгих поставки приватности су кључни кораци ка заштити деце на интернету.