

Najzastupljeniji tipovi zloupotreba u digitalnom okruženju

Svetlana Aleksić, psiholog, koordinator projekta
“Nasilje-Ne,hvala!”



Co-funded by the
Erasmus+ Programme
of the European Union

Cyberbullying (sajberbuljing/sajberzlostavljanje)

Uglavnom je prisutan među mladima i može uključivati pretnje, sramoćenje ili ponižavanje u digitalnom okruženju.

Pod ovim pojmom se često smatra vršnjačko zlostavljanje na internetu, gde pojedinac ili grupa vršnjaka ima cilj da omalovaži drugu osobu i nanese štetu njenom ugledu, ličnosti i dostojanstvu.

Doxing (doksing/targetiranje)

Podrazumeva ponašanje u okviru kojeg jedna osoba (dokser) prikuplja podatke o drugoj osobi, analizira ih i tendenciozno objavljuje s namerom da je prikaže najčešće u negativnom svetlu jer je cilj doksera da nanese štetu toj osobi.

U doxing takođe spada i objavljivanje podataka o ličnosti, kao što su adresa stanovanja ili kontakt podaci (broj telefona) kako bi se osoba uznemiravala ili joj se na drugi način nanela šteta.

Cyberstalking/Cyberbombing (sajberproganjanje)

Niz uznemiravajućih ponašanja koja su izvršena više puta i koja obično uzrokuju da žrtva trpi strah, anksioznost, poniženje i ekstremne emocionalne povrede.

Ovde spada i slanje poruka, pozivanje, slanje glasovnih poruka kako bi se osoba koja je meta napada držala u stanju konstantne uznemirenosti i straha.

Važno je naglasiti da sajberproganjanje ne mora da uključuje i direktne pretnje, već se odnosi i na one aktivnosti koje izazivaju osećaj bespomoćnosti i kontinuiranog stresa.

Hacking (neovlašćen pristup tuđim podacima)

Hakovanje predstavlja neovlašćen pristup, upadanje u tuđi elektronski uređaj ili mrežu.

Često se izvodi s namerom da se napadne i inkriminiše druga osoba, te da joj se nanese šteta putem krađe podataka ili narušavanjem njene privatnosti.

Impersonacija (imitiranje / lažno predstavljanje)

Impersonacija može da se odnosi na kreiranje lažnog profila, kao i na korišćenje tuđeg identiteta.

Svrha impersonacije jeste u tome da se u ime osobe, koja joj pribegava, prave dogovori ili kako bi se ta osoba lažno predstavljala.

Catfishing (pecanje/namamljivanje)

Termin catfishing koristi se za opisivanje situacije u kojoj se neka osoba namamljuje na susret ili u vezu, pomoću izmišljenog onlajn identiteta.

Razlika u odnosu na impersonaciju je ta što se u slučaju castfihinga treća strana namamljuje na susret ili davanje informacija.

Revenge porn (osvetničko objavljivanje eksplicitnog sadržaja)

Osvetničko objavljivanje eksplicitnog sadržaja, jeste vrsta zloupotrebe koja podrazumeva objavljivanje sadržaja bez saglasnosti osobe koja se na snimku ili fotografiji nalazi.

Počinitelj ovde koristi odnos sa žrtvom, zahvaljujući kojem je i došao do spornog sadržaja, kako bi žrtvi dalje naneo štetu.

Sextortion

Predstavlja pretnju objavljivanjem eksplicitnog materijala (informacija, fotografija) zarad iznude novca ili ponižavanja žrtve.

Ostali tipovi zloupotreba u digitalnom okruženju

Trolling(troling) - kontinuirano postavljanje, uglavnom negativnih, komentara.

DoS napadi (Denial of Services) - opterećivanje/napadanje mreže kako bi se izazvao pad sistema.

SWATTing (svoting) - prijavljivanje policiji i drugim organima, najčešće lažnih požara/bombe, u cilju izazivanja panike i straha.

HVALA NA PAŽNJI !