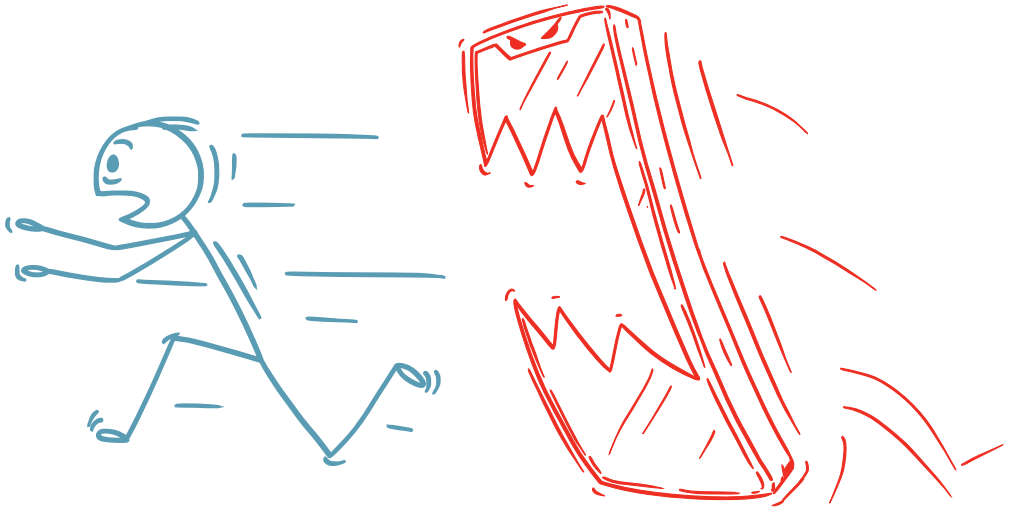
Sedam najvećih prijetnji s kojima se djeca susreću na internetu

1. Virtualno zlostavljanje

Cyberbullying ili elektroničko nasilje definira se kao „uporaba informacijskih i komunikacijskih tehnologija u svrhu namjernog, učestalog, neprijateljskog ponašanja pojedinca ili grupe s namjerom da se počini šteta drugima". Osim cyberbullyinga koje najčešće dolazi od strane njihovih vršnjaka, djecu mogu targetirati i predatori koji od njih žele novac ili seksualne usluge.

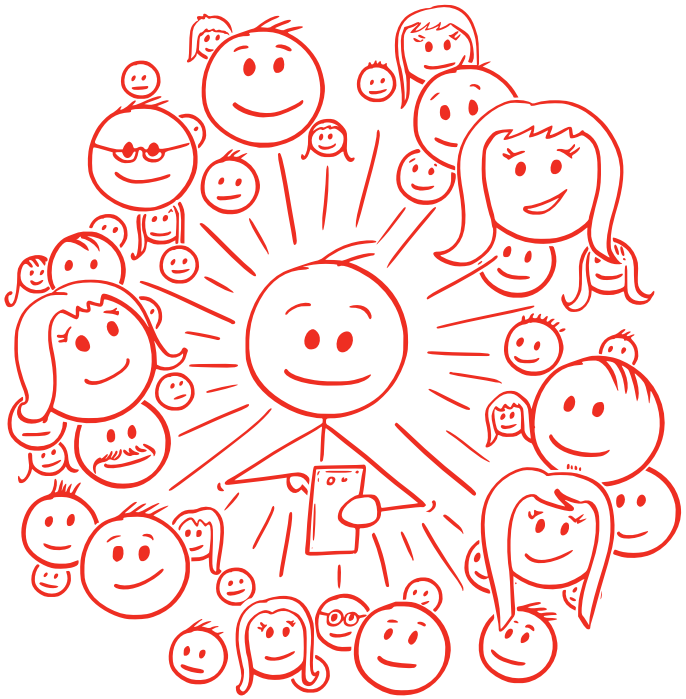
2. Virtualni predatori



Virtualni predatori manipulatori su koje djeca zbog pomanjkanja životnog iskustva najčešće ne mogu prepoznati sama. Naravno, takve situacije neprepoznavanja opasnosti ovisne su o dobi te povezanosti i komunikacijom sa starijom pouzdanom osobom. Kada su djeca uhvaćena u mrežu ucjena i uvreda virtualnih predatora, osjećaju se osamljena i bespomoćna. Za razliku od nasilja u pravom životu, djeca su uglavnom stalno online tako da od svojih nasilnika i ne mogu pobjeći.

3. Objavljivanje privatnih informacija

„Kada se nešto jednom objavi na internetu, zauvijek ostaje svima dostupno" – rečenica je koju smo mnogo puta čuli, no rijetko tko je se sjeti prije slanja ili objavljivanja fotografija, osobnih podataka ili geolokacije. Djeca su u tome još povodljivija jer zbog manjka životnog iskustva još ne razumiju granice društvene prihvatljivosti na internetu niti opasnosti koje im takve nepromišljene akcije mogu izazvati.

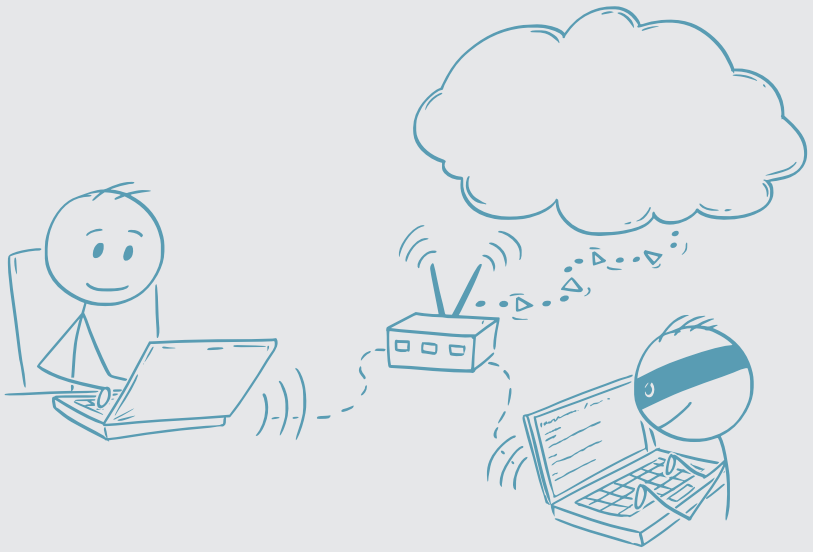


4. Krađa identiteta (phishing)

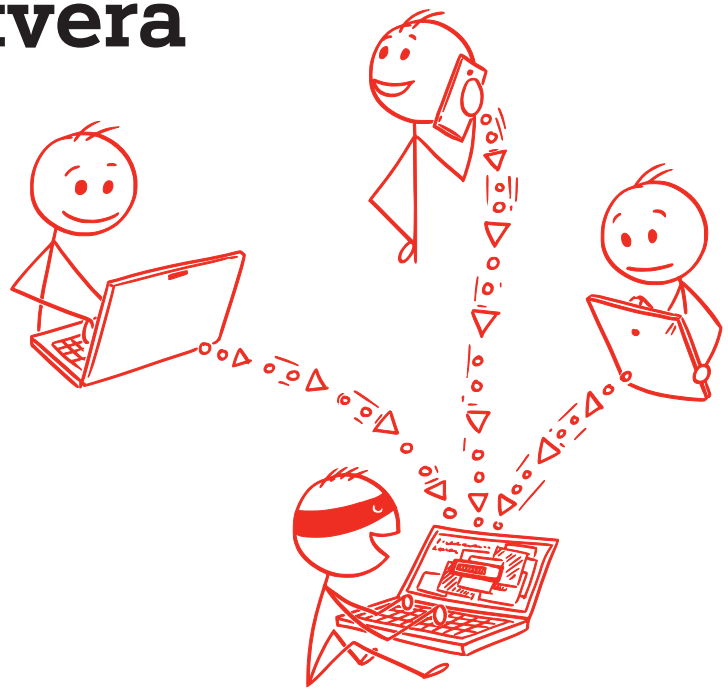
Phishing je naziv iza kojeg se kriju lažne poruke (e-mail) kojima se pokušava navesti primatelje da kliknu na zlonamjerne linkove ili privitke, a koji ih dalje vode na stranice zloćudnog web poslužitelja. Na taj način raznim manipulacijama kriminalci od korisnika žele prikupiti povjerljive podatke (korisnička imena, lozinke, brojeve i podatke s bankovnih kartica) kako bi ostvarili korist. Takve zloćudne web stranice obično se lažno (i vizualno) predstavljaju kao renomirane bankarske institucije, servisi za plaćanje, servisi za izravnu komunikaciju ili društvene mreže. U svrhu phishinga često se targetiraju stranice koje su popularne među djecom te se kroz njih prikupljaju adrese e-pošte ili imena djece i njihovih prijatelja. Ako djeca imaju profile na društvenim mrežama ili se na njih prijavljuju preko roditeljskih profila, ono što objave potencijalno može biti opasno jer (nenamjerno) objavljeni privatni podatci mogu poslužiti za krađu identiteta. Slanje takvih linkova i privitaka porukama naziva se smishing.

5. Nasjedanje na prevare

Osim zlonamjernih linkova i privitaka, ponekad se kriminalci žele dočepati i financijske koristi – uglavnom obećavajući djeci nešto ako im zauzvrat daju broj kreditne kartice roditelja ili slično. Društvene su mreže posebno opasne zbog činjenice da su takve poruke koje sadrže prijevaru dobivene od „prijatelja" s društvene mreže, a tim su „prijateljima" zapravo oteti računi, ali to (još) ni jedna strana ne zna. Zato takve poruke imaju određeni kredibilitet i rijetko tko u njih posumnja iz prve.



6. Nenamjerno preuzimanje zlonamjernog softvera



Nekada nije potrebna intervencija trećih osoba da djeca preuzmu zlonamjerni softver (malware) na svoje ili roditeljsko računalo, jer takvi softveri dolaze u obliku privlačnih online igara koje mogu zaintrigirati djecu. U tim ih slučajevima ona, zbog neznanja i radoznalosti, nenamjerno preuzmu.

7. Objave koje proganjaju dijete kasnije u životu

Ono što vaše dijete objavi na internetu kasnije je gotovo nemoguće obrisati. Mladi ljudi uglavnom ne razmišljaju o tome što bi njihovi budući profesori, poslodavci, šefovi ili potencijalni životni partneri u dalekoj budućnosti mogli misliti o njihovim mladenačkim tekstovima, video i foto sadržajima koje objavljuju na svojim profilima na društvenim mrežama, forumima, portalima i blogovima.

U suradnji s:

Poliklinikom za zaštitu djece i mladih Grada Zagreba
Plavim telefonom
Centrom za nestalu i zlostavljanu djecu