

OUCH!

U OVOM IZDANJU...

- Okolnosti
- Rizici
- Edukacija dece

Edukacija dece u vezi sajber bezbednosti

Okolnosti

Zapanjujuće je na koliko mnogo načina danas deca na Internetu mogu da stupe u interakciju sa drugima. Novi društveni mediji niču kao korov, a sve je veći broj aplikacija i igara koji podrazumevaju Internet konekciju. Deca danas bukvalno odrastaju na Internetu. Pored svih prednosti takvog detinjstva, ono sa sobom nosi određene rizike. U ovom izdanju objasnićemo tri glave oblasti rizika, kad su deca u pitanju, i šta možete da uradite da ih zaštitite.

Gost urednik

Bob Rudis je „Data Scientist“ u Verizon-u , autor izveštaja istrage o ugroženosti podataka u 2015 i staratelj četvero divne dece. Bob je osmislio i vodio efikasne programe o podizanju svesti o bezbednosti informacija u mnogim Fortune 100 kompanijama. Možete ga pratiti na Twitter-u na [@hrbrmstr](https://twitter.com/hrbrmstr).

Rizici

1. **Ponašanje:** Prilikom on-line komunikacije ili interakcije u virtuelnom svetu, deca se mogu ponašati na totalno drugačiji način nego u stvarnom svetu. Odsustvo fizičke prisutnosti može stvoriti snažan osećaj anonimnosti, naročito kod dece, tako da su često u iskušenju da se izraze na način kojim mogu da povredu drugu decu, nazvan „cyberbullying“ ili „griefing“. Osim toga vaša deca mogu postati žrtva zlonamernih osoba, bilo odraslih ili duge dece.
2. **Kontakt:** Deca su danas u skoro permanentnoj komunikaciji sa drugima, bilo kroz pisanje poruka, interakciju u „on-line“ zajednicama ili igranje u virtuelnim svetovima. Odsustvo fizičkog prisustva može da uzrokuje da zaborave šta je u njihovom najboljem interesu ili da osoba, sa kojom su u komunikaciji, ne mora da bude ona za koju se predstavlja. „On-line“ grabljivci lutaju digitalnim ulicama spremni da iskoriste svaku moguću priliku i taktiku da izgrade odnos sa potencijalnim žrtvama, a da se pritom često i sami predstavljaju kao deca.
3. **Sadržaj:** Mnogo je načina na koje je danas na Internetu moguće preuzeti ili objaviti video, zvuk, sliku ili tekstualnu poruku. Veliko iskušenje i rizik za lične podatke predstavlja mogućnost da deca previše toga objave ili podele sa drugima, bilo o sebi, bilo o članovima svoje porodice, bez razumevanja posledica takvog čina. Deca često

Edukacija dece u vezi sajber bezbednosti

ne razumeju ni rizike krađe identiteta ili infekcija štetnim softverom, kao i druge rizike koje sa sobom nosi društveni inženjering. Konačno, živimo u dobu u kome ne postoji mogućnost za „opoziv“ kada se nešto objavi na Internetu ili podeli sa drugima. Deca mogu da misle da su Kik, Instagram, Snapchat i ostale vrste postova i objava prolazne, ali takve stvari ostaju i mogu kasnije u životu da predstavljaju problem, kako za njih, tako i za članove porodice.

Edukacija dece

Stvar broj jedan koju možete da uradite da bi zaštitili svoju decu je da sa njima razgovarate. Upoznajte se sa stvarima kojima se vaša dece bave na Internetu, upoznajte ih sa aktuelnim rizicima i kako da se ponašaju da bi se zaštitili.



Ključ bezbednosti vaše dece na Internetu leži u njihovom upoznavanju sa opasnostima sa kojima mogu da se suoče, i dvosmernoj komunikaciji, u kojoj ne govorite samo vi njima, nego i oni vama.

- 1. Bezbednost kod kuće:** Bez obzira na današnju globalnu mobilnost, bezbedno „on-line“ ponašanje kreće iz kuće. Što ranije krenete da razgovarate sa svojom decom, a i oni sa vama, to bolje. Organizujte redovne razgovore u vezi Internet bezbednosti, gde će te im pokazati čak i stvarne negativne događaje iz realnog života. Ako neznate šta vaša deca rade, jednostavno ih pitajte. Pretvarajte se da ste nevešti roditelj koji želi da sazna više o novim tehnologijama i kako ih oni koriste. Deci se dopada ideja da nekom budi učitelj i velika je prilika da će vam se otvoriti. Na primer, ako imaju profil na Instagram-u, pitajte ih da vam pokažu kako Instagram funkcioniše, da vam otvore nalog i da vas povežu sa sobom. Na takav način, ne samo da možete da saznate i nadgledate šta vaša deca rade, nego i da uspostavljate odnos u kome će oni lakše razgovarati sa vama. Osim toga, prilagodite, koliko je to moguće, da se sve Internet aktivnosti odvijaju u centralnim delovima vaše kuće i takođe ograničite vreme koje provode na Internetu. Ako je kućni računar na vidljivoj lokaciji, daleko su manje šanse da se deca ponašaju kako ne treba. Takođe imajte na umu i centralnu lokaciju za punjenje mobilnih telefona, uključujući i pravilo da se svi telefoni ostavljaju pre spavanja.
- 2. Bezbednost van kuće:** Kad su deca van kuće, rizik je veći. Pomozite im da razumeju da vaša sajber pravila važe uvek i svuda, a obavezno upoznajte i one kojima decu ostavljate na čuvanje sa vašim sajber pravilima. Ako imaju mobilni telefon, proverite korišćenje (vreme i protok) da bi ste se uverili da li zloupotrebljavaju situacije kada

Edukacija dece u vezi sajber bezbednosti

su van kuće. Naravno da nećete moći da prekinete sva kršenja pravila, ali će im vaše reči pasti na pamet kada dođe u pitanje njihovo pravo na mobilni telefon.

3. **Bezbednost u brojkama:** Imajte na umu da u ovom sajber nadgledanju ne treba da budete sami. Potrebno je da sarađujete sa drugim roditeljima, starateljima, rođacima, nastavnicima i prijateljima koju uvek mogu da pomognu i ukažu na potencijalno opasno i štetno ponašanje. Utičite na vašu okolinu da ide u korak sa decom i da ih podstiče na pozitivnu interakciju kad god primete bilo kakvo rizično ponašanje.

Na kraju, ako deca prave greške, tretirajte svaku kao iskustvo iz koga se uči umesto da odmah primenite disciplinske mere. Svaki put objasnite „zašto“ i podsetite ih da vi samo želite da ih zaštitite od opasnosti koje oni još nisu u stanju da vide. Stavite im do znanja da ako dožive bilo kakvu neprijatnost u Internet komunikaciji uvek mogu da vam se obrate. Postarajte se da budu slobodni i da van se obrate i ako oni učine nešto loše. Imajte na umu da je komunikacija u stvarnom svetu koju imate sa njima najbolji način da zaštitite vašu decu u digitalnom svetu.

Saznaj Više

Prijavi se na OUCH! mesečni bilten bezbednosnih saveta za korisnike računara, pristupi prethodnim OUCH! izdanjima i saznaj više o SANS rešenjima u vezi svesnosti bezbednosti informacija na našoj internet prezentaciji

<http://www.securingthehuman.org/>

Dodatne informacije

Cyber Smart: <http://www.cybersmart.gov.au/Parents.aspx>

OnGuard Online: <http://www.onguardonline.gov/topics/protect-kids-online>

Stay Safe Online: <https://www.staysafeonline.org/stay-safe-online/for-parents/raising-digital-citizens>

Securing Kids Panel:
<http://www.rsaconference.com/media/into-the-woods-protecting-our-youth-from-the-wolves-of-cyberspace>

OUCH! Objavljuje SANS Securing The Human program i distribuira se pod [Creative Commons BY-NC-ND 4.0 licencom](https://creativecommons.org/licenses/by-nc-nd/4.0/). Biltene je dozvoljeno distribuirati ili koristiti za svoj program unapređenja bezbednosne svesti uz uslov da sadržaj nije modifikovan. U vezi prevoda ili za dodatne informacije, kontaktiraj ouch@securingthehuman.org.

Redakcija: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Preveo: Nenad Varinac



securingthehuman.org/blog



[/securethehuman](https://www.facebook.com/securethehuman)



[@securethehuman](https://twitter.com/securethehuman)



[securingthehuman.org/gplus](https://plus.google.com/securingthehuman.org)