KAKO SE ZAŠTITITI

U SVIJETU INTERNETA I MOBILNIH TELEFONA

KRATKI VODIČ ZA RODITELJE
(i sve koji žele znati više u digitalnom dobu)

HAKOM | HRVATSKA REGULATORNA AGENCIJA ZA MREŽNE DJELATNOSTI

Internet i društvene mreže jako pomiču osobne granice i mijenjaju kontekst značenja privatnosti. Širenje informacija i podrške je vrlo brzo, korisno i privlačno, a internet i društvene mreže jako mijenjaju granice privatnog i onog što postaje javno. Onog trenutka kad nešto objavimo na internetu, mi zapravo više nad tim sadržajem nemamo kontrolu, a predmet naše objave prestaje biti intiman, privatan i tajan. Ovisno o tome kako nam je kreiran profil, ali i o samim osobitostima društvenih mreža, naše objave mogu vidjeti pa onda i komentirati i ljudi koje mi ne poznajemo i ne smatramo bliskim prijateljima. Upravo zbog toga, objavljivanjem slika i previše informacija o djetetu i mjestima gdje se ono kreće i boravi, čak kad to činimo u najboljoj namjeri, možemo ugroziti djetetovo pravo na sigurnost.

Najveće i najsveobuhvatnije nacionalno komparativno istraživanje o medijskim navikama djece i njihovih roditelja te sigurnosti djece na internetu provedeno je u sklopu projekta **"EU Kids Online"** 2017. U istraživanju je sudjelovalo 1017 djece u dobi od 9 do 17 godina i njihovi roditelji, pri čemu je u istraživanju sudjelovao onaj roditelj koji je bio bolje upoznat s digitalnim navikama djece. Opći cilj istraživanja bio je steći bolji uvid u navike djece pri korištenju interneta i suvremenih tehnologija, ispitati učestalost i oblike izloženosti djece uznemirujućim sadržajima i nasilju te ispitati zaštitne faktore i ulogu okoline u zaštiti i edukaciji djece i mladih od opasnosti na internetu.

14% djece susrelo uživo s osobom koju su upoznali na internetu pri čemu takve aktivnosti rastu s dobi pa je u ovoj skupini najviše mladih od 15 do 17 godina (27%), zatim djeca od 12 do 14 godina (12%) i na kraju 3% najmlađe djece u dobi od 9 do 11 godina. Pritom je tek 5% roditelja svjesno da su se njihova djeca susrela uživo s osobom koju su upoznali na internetu.

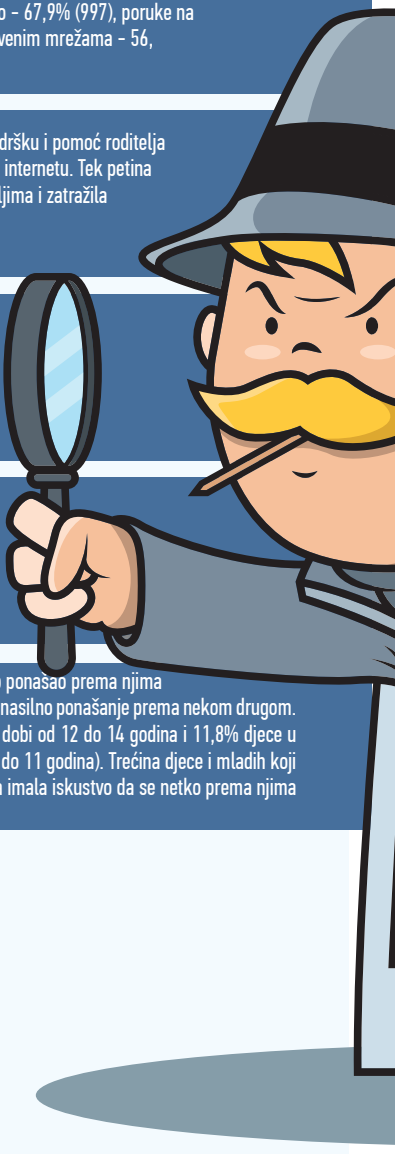
82,1% roditelja smatra da je djeci potrebno postaviti pravila o korištenju interneta, a čak 62,6% roditelja smatra da je djecu potrebno nadzirati prilikom korištenja interneta. Pritom, roditelji najviše provjeravaju sljedeće sadržaje: koje je internetske stranice dijete posjetilo - 67,9% (997), poruke na e-mailu ili drugim aplikacijama 58,5% (997), profil na društvenim mrežama - 56, 9% (989), aplikacije koje je kupilo - 42,8% (972).

1/2 Gotovo polovina djece nikad ili gotovo nikad nije zatražila podršku i pomoć roditelja u vezi situacija i problema koji su ih uznemirili dok su bili na internetu. Tek petina djece je navela da je često ili vrlo često razgovarala s roditeljima i zatražila njihovu pomoć i podršku kada nisu nešto znali ili su doživjeli uznemirujuće iskustvo.

7. Svako sedmo dijete u dobi od 9 do 17 godina u posljednjih se godinu dana susrelo s online prijateljem, odnosno osobom koju je upoznalo preko interneta. Većina djece se susrela s osobom svojih godina, dok se svako deseto dijete susrelo s osobom starijom od sebe.

1/2 Gotovo polovina djece otišla je na sastanak uživo s 1 do 2 online prijatelja, dok je 1/10 njih imala susrete s više od 10 online prijatelja.

7% djece u dobi od 9 do 17 godina imalo je iskustvo da se netko ponašao prema njima na povređujući ili neugodan način, dok je 4,5% djece priznalo nasilno ponašanje prema nekom drugom. Elektroničkom su nasilju više izložena starija (6,4% djece u dobi od 12 do 14 godina i 11,8% djece u dobi od 15 do 17 godina), nego mlađa djeca (4% u dobi od 9 do 11 godina). Trećina djece i mladih koji priznaju nasilno ponašanje prema drugima (33,3%) je i sama imala iskustvo da se netko prema njima ponašao na povrjeđujući ili neugodan način.



NEMOJTE IĆI SAMI NA SUSRETE S NEPOZNATIM OSOBAMA KOJE STE UPOZNALI ONLINE.

Istraživanje je pokazalo dosta razočaravajuće rezultate kad je u pitanju podrška nastavnika u korištenju interneta među djecom. Svako treće dijete istaknulo je da nastavnici nikada ili gotovo nikada nisu razgovarali s njima o tome što rade na internetu niti što bi učinili kada bi ih nešto mučilo na internetu, niti su im pomogli kada im je na internetu nešto bilo teško napraviti ili pronaći. Svako četvrto dijete je reklo da im nastavnici nikada ili gotovo nikada nisu predložili sigurne načine korištenja interneta, a njih čak 42,1% priznalo je da im nastavnici nikada ili gotovo nikada nisu pomogli kada ih je nešto mučilo na internetu. Pritom su rezultati pokazali da podršku u korištenju interneta od strane nastavnika češće dobivaju starija, nego mlađa djeca.

OSIGURAJTE OTVOREN I ISKREN ODNOS S VAŠOM DJECOM I POTIČITE IH DA UVIJEK TRAŽE POMOĆ RODITELJA ILI ODRASLE OSOBE KOJOJ VJERUJU KADA IH UZNEMIRI NEŠTO U VIRTUALNOM SVIJETU ILI NAIĐU NA NEPRIMJEREN SADRŽAJ.

IZVOR: HRKIDS.ONLINE

INTERNET IMA **DOBRE** I KORISNE, A ISTO TAKO I LOŠE STRANE.

Djecu treba naučiti i razvijati vještinu uspješnog korištenja interneta te će tada moći uspješno koristiti njegove mogućnosti i prednosti, osobito pri stjecanju znanja.

DOBRE STRANE SU:

- razvijanje vještina učenja
- motiviranje i poticaj za učenje
- brza i laka dostupnost najrazličitijih informacija – materijali za školu i učenje, vijesti, različiti sadržaji vezani uz hobije i interese
- druženje s prijateljima preko društvenih mreža
- mogućnost brze i lake komunikacije, razmjene iskustava, mišljenja i informacija
- zvuk, animacije, video zapisi i drugi dinamični elementi čine učenje zanimljivijim
- može se pristupiti onome što učiš s bilo kojeg mjesta koje ima pristup internetu
- stjecanje novih znanja (online škole)
- videopozivi prema obitelji i prijateljima koje rijetko viđaju (provođenje vremena)

LOŠE STRANE SU:

- zlostavljanje putem interneta, lažno predstavljanje
- narušena sigurnost, sadržaj nije primjeren dobi djeteta
- djeca pristupaju društvenim mrežama u dobi koja nije primjerena
- zloupotreba podataka
- širenje mržnje među drugima

NASILJE NE VRŠI TEHNOLOGIJA VEĆ LJUDI KOJI SE SLUŽE S NJOM.

Djeca većinu svog vremena provode u socijalizaciji na internetu, nego u stvarnom kontaktu s vršnjacima te je stoga neodgovorno roditeljsko ponašanje zanemariti to područje ili smatrati da je to nešto za mlade. Novi mediji zahtijevaju od roditelja preuzimanje novog, vrlo značajnog i izazovnog odgojnog zadatka. Roditelji su dužni pojasniti djetetu što znači biti nasilnik na internetu i informirati ga o posljedicama takvog oblika nasilja, naučiti ga odgovornom ponašanju na internetu i kritičkom razmišljanju pri korištenju novih medija.

Ukoliko se roditelj ne služi društvenim mrežama i ne razumije ih, manja je vjerojatnost da će dijete ozbiljno shvatiti roditeljski savjet, odnosno smatrat će da roditelj pretjeruje s brigom i upozorenjima.
Roditelji mogu zamoliti djecu da im pokažu i nauče ih kako funkcioniraju društvene mreže. Kad se dijete nađe u ulozi učitelja osjećat će se važno i odraslo, a to će stvoriti odličnu priliku za razgovor s djetetom o onome što se događa na internetu.

ZAŠTITA **OSOBNIH PODATAKA** NA INTERNETU

PRIJE REGISTRACIJE NA DRUŠTVENOJ MREŽI VAŽNO JE PROČITATI POSTAVKE PRIVATNOSTI.

Od 25. svibnja 2018. zaštita osobnih podataka, u realnom i virtualnom svijetu, postala je ozbiljnija i značajnija. Tog je dana u Europskoj uniji započela potpuna primjena Opće uredbe o zaštiti podataka (poznatije kao skraćenica GDPR) koja svima koji prikupljaju i obrađuju osobne podatke nameće nova pravila.

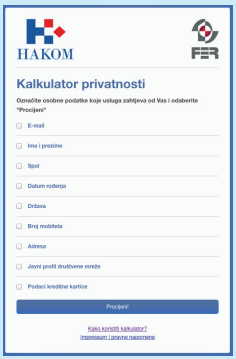
Svatko mora prije samog prikupljanja podataka biti upoznat s osnovnim informacijama o tome tko i u koju svrhu prikuplja podatke, do kada će ih čuvati i obrađivati, kome će biti dostavljeni te koja su njegova prava.

Prije ostavljanja bilo kakvih osobnih podataka na internetu i društvenim mrežama dobro je proučiti pravila privatnosti, opće uvjete i sva druga upozorenja. Nakon javne objave nekog podatka, taj podatak zapravo više nije naše vlasništvo.

Ako se za pristup određenim aplikacijama ili uslugama traži davanje suglasnosti/privole, dobro proučimo za što dajemo suglasnost (npr. za lociranje) i imajmo na umu da je uvijek sigurnije dati što manje osobnih podataka.

TREBA IMATI NA UMU DA GDPR PROPISUJE DA U SLUČAJU NUĐENJA USLUGA INFORMACIJSKOG DRUŠTVA (NPR. INTERNET TRGOVINE), PRIVOLU ZA OBRADU OSOBNIH PODATAKA DJETETA MLAĐEG OD 16 GODINA MOŽE DATI SAMO RODITELJ ILI SKRBNIK!

KALKULATOR PRIVATNOSTI



Provjerite potencijalni rizik za vlastitu privatnost prilikom korištenja interneta i davanja osobnih podataka. Uobičajeno je da se u većini slučajeva traži registracija tijekom koje korisnik mora predati svoje osobne podatke, najčešće e-mail adresu, ime i prezime. **Putem aplikacije Kalkulator privatnosti možemo se educirati,** a navedena aplikacija potaknut će nas na razmišljanje o problemima sigurnosti i privatnosti na internetu **http://privatnost.hakom.hr/index.php**

UPOZORENJE

DJECI, MLADIMA I RODITELJIMA

- Nemojte javno objavljivati i razmjenjivati osobne i intimne podatke (lokaciju, fotografije, datum rođenja, adresu i slično)
- Ne objavljujte tuđe podatke (npr. fotografije prijatelja i članova obitelji) bez suglasnosti te osobe

RODITELJIMA,

- Nemojte objavljivati osobne podatke i fotografije djece na internetu
- Ne objavljujte lokacije i mjesta gdje vaša djeca borave (škola, vrtići i slično)

Često objavljujemo sadržaj, ali iz tog razloga moramo biti svjesni da objavljeni sadržaj može zauvijek ostati "negdje u nekom virtualnom prostoru" pa je moguće da jednom u budućnosti djetetu neće biti ugodno zbog njegovih slika i sadržaja koji su bili dostupni roditeljevim prijateljima, ali i drugim ljudima.

USLUGA "RODITELJSKE ZAŠTITE"

Usluga „Roditeljska zaštita" nudi mogućnost zabrane pristupa neprimjerenim internetskim sadržajima za djecu. Zaštita osigurava filtriranje internetskog sadržaja, ograničavanje poziva ili slanje poruka prema nepoznatim brojevima ili roditelji sami kreiraju popis brojeva s kojima dijete može komunicirati.

Ako primamo SMS ili MMS poruke sa sadržajem neprimjerenim djeci i namijenjene isključivo odraslima, o tome možemo obavijestiti svoga operatora ili prijaviti primitak takve poruke na adresu elektroničke pošte **nezeljeni.sms@hakom.hr**. Brojevi s kojih se šalju takve poruke će se nakon provjere u najkraćem mogućem roku blokirati.

Mogućnost isključenja korištenja pojedinih usluga. Zabrana slanja i/ili primanja SMS i MMS poruka u okviru usluge s posebnom tarifom (6xx xxx, 8xx xxx i sl.) može se besplatno zatražiti od operatora. **Moguće je postaviti zabranu odlaznih poziva nakon dogovorenog limita potrošnje.** Novčani limit potrošnje za usluge s posebnom tarifom koje su namijenjene djeci (iznos 50,00 kn).

Roditelji, možete ograničiti vrijeme koje dijete provodi na mobitelu uz besplatne aplikacije. Osim toga, aplikacije nude i opciju praćenja djetetovih aktivnosti na uređaju. Svakako razgovarajte s djetetom prije nego instalirate aplikaciju i zajedno dogovorite pravila.

Svaki operator koji pruža i usluge televizije omogućava roditeljsku zaštitu koja se može aktivirati po potrebi i željama korisnika. Omogućavanje zabrane pristupa gledanju neprimjerenih TV programa i filmova, poput pornografskih ili nasilnih sadržaja.

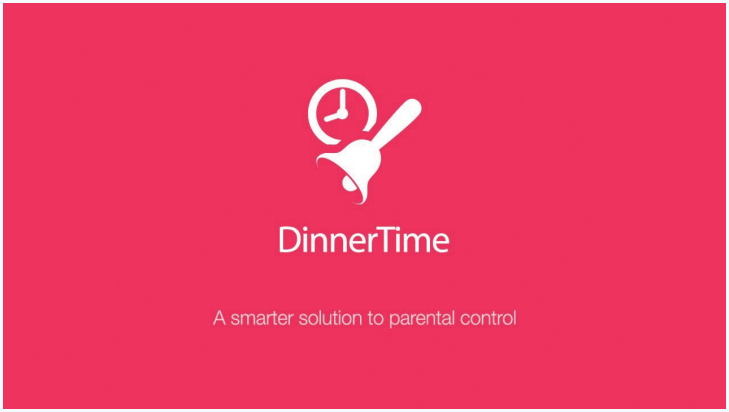
Pravila trebaju uzeti u obzir dob djeteta i definirati doba dana te ukupno vrijeme koje dijete smije provesti na računalu ili mobitelu, vrstu igrice ili aplikacije koje će koristiti. Kod mlađe djece preporučljivo je koristiti opcije roditeljskog nadzora i filtriranja sadržaja, ali svakako djecu informirajte o postavkama filtera.

POSTAVITE **OKVIRNA PRAVILA** U DOGOVORU S DJETETOM

Ukoliko dijete/tinejdžer osjeti prevelik utjecaj na svoju privatnost ili pomisli da ga se „špijunira“, izgubit će povjerenje u roditelje te će lako naći način da od roditelja sakrije ono što ne želi da se zna. Ova situacija može biti jako opasna u slučaju da se dijete ili tinejdžer zaista nađe u problemu jer se zbog narušenog povjerenja neće htjeti obratiti roditelju za pomoć.

Roditelji mogu ograničiti vrijeme koje dijete provodi na mobitelu uz besplatne aplikacije. Osim toga, aplikacije nude i opciju praćenja djetetovih aktivnosti na uređaju međutim treba uzeti u obzir djetetovo pravo na privatnost i što je dijete starije, manje su primjerene.

DINNER TIME aplikacijom upravlja se putem roditeljevog mobitela koji može biti Android, ili iPhone, a djetetov mobitel mora biti Android. Moguće je u bilo kojem trenutku uključiti pauzu od korištenja uređaja; ograničiti ukupno vrijeme koje dijete može provesti koristeći uređaj ili određene aplikacije.



KIDS PLACE aplikacija stvara sučelje za dijete i omogućuje sortiranje aplikacija koje dijete smije koristiti na mobitelu. Onemogućuje preuzimanje novih aplikacija, korištenje telefonskih poziva, SMS poruka i ostalih radnji koje mogu izazvati trošak. Za izlazak iz Kids Place aplikacije i ulazak u roditeljsko sučelje potreban je PIN koji roditelj sam bira. Aplikacija je prikladna za mlađu djecu.

METODE **ELEKTRONIČKOG NASILJA I UZNEMIRAVANJA**

Cyberbulling (elektroničko nasilje)-djeca se najčešće zlostavljaju putem mobitela i društvenih mreža

Elektroničko nasilje uključuje različite oblike napada na pojedinca, slanje prijetećih poruka, osnivanje grupa koje podržavaju mržnju na društvenim mrežama. Osim zajedničkih karakteristika koje imaju „tradicionalno" i „moderno" vršnjačko nasilje poput agresivnosti, namjere da se nekoga povrijedi te nemogućnosti žrtve da se obrani, vršnjačko nasilje putem interneta sa sobom nosi nove opasnosti za žrtvu. Jedna od najvažnijih karakteristika vršnjačkog nasilja putem interneta jest činjenica da ono nikad ne prestaje.

Od udaraca ili uvreda „licem u lice" žrtva može pobjeći u sigurnu zonu u kojoj tome neće biti izložena. Međutim, kada je riječ o nasilju putem interneta, uvrede, fotografije, video zapisi i agresija ostaju na internetu i svima su dostupni. Nadalje, počinitelj nasilja na internetu ima prividni osjećaj anonimnosti, puno snažniji nego što je to slučaj kod nasilja u stvarnom svijetu. S druge strane, počinitelj za vrijeme nasilnog ponašanja putem interneta nije u mogućnosti vidjeti reakcije svoje žrtve, zbog čega njegovo ponašanje može postati još agresivnije i bezobzirnije.

NEKE OD METODA ELEKTRONIČKOG NASILJA KOJIMA SE ZLOSTAVLJAČI SLUŽE SU:

- Grubo online sukobljavanje, uznemiravanje, ogovaranje i klevetanje i socijalno isključivanje.
- Lažno predstavljanje
- Uzimanje tuđeg identiteta i slanje poruka i drugih sadržaja u tuđe ime.
- Iznuđivanje i širenje povjerljivih informacija
- Javno objavljivanje podataka koje je žrtva u povjerenju poslala počinitelju nasilja. Također, počinitelj može manipulirati žrtvom da napiše nešto privatno koje onda javno objavljuje ili dijeli dalje bez dopuštenja.
- Prijetnje i uhođenje
- Opetovano slanje prijetećih poruka te neprestani pokušaji uspostavljanja i nastavljanja neželjenog kontakta zbog kojih se žrtva počinje bojati za vlastitu sigurnost i dobrobit. Posebno je izraženo prilikom komunikacije s nepoznatim osobama i u slučajevima seksualnog nasilja putem interneta
- Videosnimanje
- Snimanje ili fotografiranje u situacijama koje su za djecu ponižavajuće ili neugodne; izazivanje i snimanje tučnjave ili drugih nasilnih sadržaja te njihovo širenje.
- Izmjena fotografija
- Izmjena osobnih fotografija bez dozvole i objava na internetu.

SLJEDEĆI ZNAKOVI U OSNOVNOJ ŠKOLI I KOD KUĆE MOGU UKAZIVATI DA JE DIJETE UKLJUČENO U NASILJE MEĐU DJECOM, A MOGU BITI PRISUTNI I KOD DJETETA KOJE JE UKLJUČENO U ELEKTRONIČKO NASILJE

(Rivers, Duncan, Besag, 2009, prema Križan, 2018.).

RODITELJI

Znakovi koji ukazuju da je dijete možda doživjelo vršnjačko nasilje:

- učestala tišina
- povlačenje iz obiteljskih interakcija
- vidljiva tuga
- povlačenje od prijatelja i od aktivnosti u kojima je prije uživalo
- učestaliji izostanci iz škole (žaljenje na glavobolje i bolove u trbuhu)
- loš školski uspjeh (niže ocjene)
- gubitak apetita
- poremećaji spavanja (uključujući mokrenje u krevet)
- informacije iz škole o izgubljenim domaćim zadaćama ili problemima u ponašanju kao što su tučnjave s drugim učenicima
- prestaje koristiti računalo ili mobitel ili povećanje vremena provedenog na internetu u odnosu na prije
- čini se nervozno ili razdražljivo kada koristi računalo ili mobitel
- spominje nepoznate osobe
- pridavanje sve veće važnosti aktivnostima i osobama na internetu
- zatvaranje stranica, chatova i/ili skrivanje mobitela kada roditelji uđu u sobu ili kada se druga osoba približi
- stres prilikom čitanja poruka, odnosno primanja različitih sadržaja
- izbjegavanje razgovora o uporabi računala i interneta
- brisanje korisničkih računa ili otvaranje puno novih
- puno novih kontakata na mobitelu i/ili društvenim mrežama

UČITELJI

Znakovi koji ukazuju da je učenik/učenica možda doživio/doživjela vršnjačko nasilje:

- izbjegavanje kontakta očima i vidljiva tuga
- pojava nekontroliranih izljeva bijesa ili frustracije
- promjene u obrascima ponašanja s prijateljima i aktivnostima za vrijeme odmora
- nedostatak angažmana u razrednim ili grupnim aktivnostima u kojima je prethodno bio/bila aktivno angažiran/a
- učenici ga/je ismijavaju kada govori
- pridavanje manje pažnje školskom i domaćem radu

KAKO RODITELJI MOGU POMOĆI?

01 Razgovarajmo sa svojim djetetom. Otvoreno i često, čak i kad ne sumnjamo da postoji problem. Pokažimo mu da nam može vjerovati i da se na nas uvijek može osloniti. Razgovarajmo o internetu i ponašanju na društvenim mrežama. Međusobno poštovanje i uvažavanje su temelj svakog odnosa – online i offline. Objasnimo djetetu da ne smije postojati razlika između ponašanja u stvarnom i virtualnom svijetu – u oba slučaja vrijedi pravilo da druge ljude trebamo uvažavati i poštivati i prema njima se primjereno ponašati te od njih očekivati isto.

02 Budimo upoznati s ponašanjem svog djeteta na internetu. Kao što želimo znati s kim naše dijete provodi vrijeme u stvarnom svijetu, trebali bi znati i s kim provodi vrijeme u virtualnom svijetu.

03 Zamolimo dijete da nam pokaže koje stranice posjećuje i što tamo radi. Poučimo ga da u virtualnoj komunikaciji uvijek treba biti oprezan. Računalo držimo na pristupačnom mjestu gdje možemo imati nadzor nad djetetovim aktivnostima i odredimo vrijeme koje može provesti na internetu. Potaknimo dijete da koristi računalo za učenje i druženje. Dajmo mu do znanja da nam se može obratiti svaki put kad na internetu primijeti nešto neprimjereno ili uznemirujuće.

04 Roditeljima često nije lako prihvatiti mogućnost da je njihovo dijete počinitelj elektroničkog nasilja. Saznajte što se točno dogodilo i koje je uređaje, aplikacije ili društvene mreže dijete koristilo. Nikada nemojte prijetiti, osuđivati i vrijeđati dijete.

05 Objasnimo djetetu da svako zlostavljanje, bilo fizičko ili verbalno, uzrokuje bol drugoj osobi. Pomognite djetetu da razvije suosjećanje i da pokuša zamisliti kako bi se ono osjećalo ukoliko bi bilo izloženo nasilju. Ponudite djetetu pomoć pri promjeni i ispravljanju ponašanja.

06 Vrlo često zlostavljano dijete postaje zlostavljač. Seksualno uznemiravanje i zlostavljanje je protuzakonito i žrtva nikada nije kriva za ono što se dogodilo.

OPASNOSTI NA INTERNETU

Računalni kriminalci se koriste malicioznim (zlonamjernim, štetnim) programima pomoću kojih zaobilaze zaštitu naših računala kako bi pristupili našim računalima i podacima.

Dnevno se otkrije nekoliko stotina tisuća novih malicioznih datoteka, a računalne obrane jednostavno ne mogu držati korak s takvom bujicom zlonamjernih programa. Zbog toga je potrebno biti upoznat s opasnostima na internetu – Edukacija je najbolja obrana!

Putem elektroničke pošte, slanjem poruka za koje se na prvi pogled čini da dolaze od neke poznate tvrtke (Facebook, Ebay, Paypal, Snapchat i drugi) ili sličnim načinima. Svrha takvih poruka je da nas potaknu na unošenje svojih osobnih podataka u aplikaciju čime kriminalcima dajemo pristup našim podacima. A jednom, kada imaju podatke o nama, oni su u mogućnosti načiniti značajnu štetu, primjerice uzeti kredit u naše ime, obaviti kupnju s našim karticama, predstavljati se kao mi i slično.

Zlonamjerne poruke mogu doći i s adresa koje nam se na prvi pogled čine poznate. Često računalni kriminalci pribjegavaju tome da provale i preuzmu nečiju e – mail adresu i pošalju lažne poruke svim ljudima koje nađu u imeniku.

AKO PORUKA DOLAZI OD NEPOZNATE OSOBE NEMOJMO KLIKNUTI NA LINK ILI OTVORITI PRILOG (ATTACHMENT). ČAK I AKO JE OD POZNATE OSOBE - BUDIMO OPREZNI!

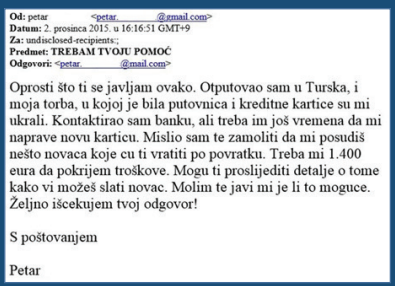

From: **Skype Notify** <gaetano@pmw.de>
Date: 20 November 2015 at 00:25
Subject: Deferred messages priming
To:

Skype

Deferred message.

View messages

Yours truly
Skype support


Od: petar <petar.@gmail.com>
Datum: 2. prosinca 2015. u 16:16:51 GMT+9
Za: undisclosed-recipients:;
Predmet: TREBAM TVOJU POMOĆ
Odgovori: <petar.@mail.com>

Oprosti što ti se javljam ovako. Otputovao sam u Turska, i moja torba, u kojoj je bila putovnica i kreditne kartice su mi ukrali. Kontaktirao sam banku, ali treba im još vremena da mi naprave novu karticu. Mislio sam te zamoliti da mi posudiš nešto novaca koje cu ti vratiti po povratku. Treba mi 1.400 eura da pokrijem troškove. Mogu ti proslijediti detalje o tome kako vi možeš slati novac. Molim te javi mi je li to moguce. Željno iščekujem tvoj odgovor!

S poštovanjem

Petar

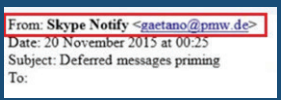
SAVJET

U SLUČAJU DA PRIMIMO SLIČNU PORUKU NIJE PREPORUČLJIVO KLIKNUTI NA LINK VEĆ U PREGLEDNIKU UNIJETI ADRESU SERVISA, NPR. www.facebook.com, ULOGIRATI SE I PROVJERITI ČEKAJU LI NAS DOISTA PROPUŠTENE PORUKE

KAKO PREPOZNATI LAŽNU PORUKU?

Neki od znakova po kojima se može prepoznati da je poruka lažna:

- ne obraća se osobno nama već počinje nekim općenitim pozdravom npr. **„Hi there“**, ili **„Hey you“** ili **„Bok!”**,
- poruka ima gramatičke pogreške (često je slučaj da nam se pošiljatelj obraća u pogrešnom licu),
- ime servisa i adresa s koje piše da je poruka došla nisu isti,


From: **Skype Notify** <gaetano@pmw.de>
Date: 20 November 2015 at 00:25
Subject: Deferred messages priming
To:

- u gornjem primjeru poruka izgleda kao da je došla od Skype-a no Skype ima domenu @skype.com, a ova poruka je došla s@pmw.de

KAKO ZAŠTITI E - MAIL ADRESU, TWITTER RAČUN I SLIČNO?

Koristimo različite lozinke za servise na internetu (nemojte koristiti istu lozinku za e - mail adresu, Facebook i druge stranice koje posjećujete). Kako ne bi pamtili stotine lozinki preporuča se poslužiti programom za upravljanje lozinkama.

Popularne stranice i servisi poput Facebook-a, Google-a i Twittera nude mogućnost tzv. potvrde u dva koraka (Two Step Verification), koja štiti korisnički profil ili e-mail adresu od neovlaštenog upada jer šalje dodatni kod na naš mobitel koji treba unijeti ukoliko se prijavljujemo s dotad nepoznatog uređaja.

Budimo oprezni kad nas putem društvenih mreža kontaktiraju nepoznate osobe i na oprez potičimo i djecu. Prije nego ih prihvatimo za prijatelje provjerimo jesu li to zaista osobe za koje se predstavljaju. To možemo učiniti i tako da uzmemo profilnu fotografiju i unesemo ju u Google pretraživač jer prevaranti često koriste tuđe fotografije za lažne profile
< upute za pretraživanje koristeći fotografije: Kada smo na Google pretraživaču prijeđemo na pretraživanje po slikama, kliknemo na ikonicu fotoaparata u rubu tražilice, odaberemo tab "Prenesite sliku" i iskoristimo fotografiju s profila za pretraživanje. > Ako istu fotografiju pronađemo na više različitih mjesta, pod jednim ili više različitih imena – sve nam je jasno. Netko se ne predstavlja svojim pravim imenom!

PRIJEVARE PUTEM INTERNETA

Internet je mjesto s puno zanimljivih informacija, no kako ga svi koristimo za pretraživanje ili komunikaciju, često ne razmišljamo gdje sve ostavljamo svoje osobne podatke poput e - mail adrese. To je jedan od razloga zbog kojeg ćemo, prije ili kasnije, biti meta onih koji žele zaraditi na nama ili nas žele iskoristiti. Takve osobe koriste internet i kao sredstvo upoznavanja sa djecom, radi uspostavljanja komunikacije i odnosa, i taj odnos zloupotrebljavaju s ciljem da djecu seksualno uznemiravaju i zlostavljaju.

Ako dobijemo ponudu kako ćemo nešto dobiti besplatno trebamo razmisliti je li to vrijedno ostavljanja osobnih podataka. Naime, drevna mudrost kaže: „Ne postoji takva stvar kao što je besplatan ručak". Drugim riječima, ako nešto zvuči predobro da bi bilo istinito – vjerojatno nije istinito! **TO POSEBNO TREBA OSVIJESTITI DJECI!** Internet prijevare se također mogu dogoditi i putem aplikacija za komunikaciju poput **VIBERA**, **WHATSAPP-a** ili drugih, gdje dobijemo poruku s poveznicom i tekstom koji nas informira da smo nešto osvojili ili da samo trebamo posjetiti poveznicu kako bi preuzeli nagradu, video ili neki drugi sadržaj. Budimo oprezni kada u svijetu nastanu situacije koje odjekuju po medijima – bilo da se radi o slavnim osobama, terorističkim napadima ili humanitarnim akcijama – kriminalci često koriste takve situacije za slanje elektroničke pošte u kojoj će vas pokušati nagovoriti da otvorite određenu stranicu ili skinete neku datoteku. Djeca se najčešće nagovaraju da otvore neku stranicu na kojoj ih „čeka" nagrada, a koja, naravno, ne postoji.

Dodatan oprez potreban je i kod instaliranja raznih aplikacija, bilo na pametnom telefonu ili Facebook-u. Provjerimo kojim sve osobnim podacima aplikacija traži pristup na našem uređaju. Ako su zahtjevi nerazumni, pa tako npr. aplikacija naziva „Kalkulator" zatraži pristup našim fotografijama i kontaktima, ne bi je trebali preuzeti! Osvijestite i djecu da ne preuzimaju bilo kakve aplikacije, odnosno da ih zajednički pregledate i prokomentirate prije same instalacije i korištenja.

Kako nas netko na internetu može pokušati prevariti?

http://privatnost.hakom.hr/catindex_hr.php?showcat

SAVJET

U TAKVIM SITUACIJAMA DOBRO JE DRŽATI SE INTERNETSKIH STRANICA KOJE I INAČE REDOVITO POSJEĆUJEMO. VIJESTI NA NJIMA BIT ĆE NAJVJEROJATNIJE PROVJERENE I SIGURNIJE NEGO DRUGDJE. NE NASJEDAJMO NA PODVALE!

DRUŠTVENE MREŽE I PROGRAMI ZA RAZMJENU PORUKA

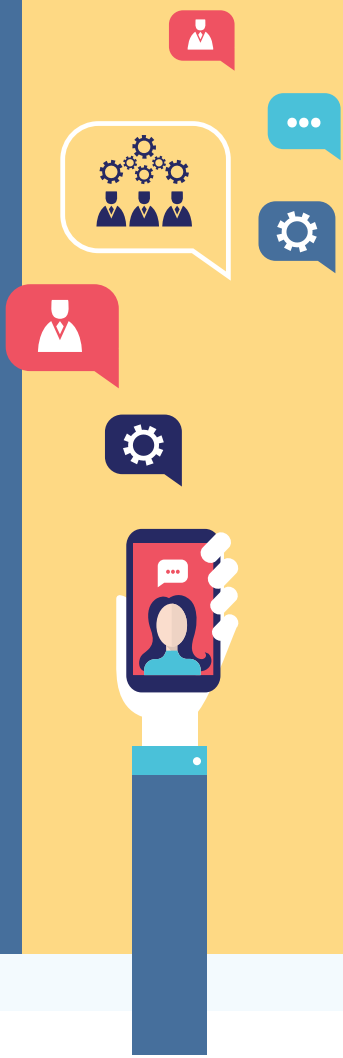
Današnja djeca i mladi teško mogu zamisliti život bez svakodnevnog korištenja društvenih mreža. Pravila lijepog ponašanja na društvenim mrežama prilagođavaju se novim tehnologijama, ali ono staro pravilo, koje vrijedi i u stvarnom životu, vrijedi u svakoj prilici:

"PONAŠAJMO SE PREMA DRUGIMA ONAKO KAKO ŽELIMO DA SE DRUGI PONAŠAJU PREMA NAMA."

SAVJET

NETIQUETTE – OPĆA PRAVILA SIGURNIJEG KORIŠTENJA DRUŠTVENIH MREŽA I PROGRAMA ZA RAZMJENU PORUKA:

- što je nezakonito u stvarnom životu nezakonito je i na internetu. Nemojmo se zavaravati misleći da se možemo skriti iza izmišljenog nadimka.
- ne ostavljajmo privatne informacije, bilo na fotografijama bilo u opisima
- ne otkrivajmo svoju lokaciju ako nije potrebno, posebno privatne lokacije,
- osigurajmo da se lokacija sa fotografije ne može otkriti korištenjem informacija s fotografije
- ne koristimo oznake (hashtags #) koje mogu otkriti privatne podatke ili lokaciju npr. #Ulica113
- ne dijelimo nasilne ili nepristojne fotografije. Pripazimo što šaljemo u svijet. Ne samo što stvaramo sliku o sebi već utječemo i na druge.
- ne sudjelujmo u nasilju putem interneta. Ne omalovažavajmo i ne vrijeđajmo.
- roditeljima se ne preporuča dijeliti fotografije svoje djece, no, ako ih dijelimo, ograničimo tko ih može vidjeti
- ako koristimo javni ili tuđi uređaj za pristup internetu ne zaboravimo se odjaviti s aplikacija koje koristimo
- način komuniciranja potrebno je prilagoditi drugom korisniku ili grupi korisnika kako bi razmjenjivanje informacija uspjelo.
- proučimo postavke za sigurnost i privatnost. Maksimalno otežajmo neželjeno širenje naših privatnih informacija.
- poštujmo privatnost - kako vlastitu, tako i ostalih korisnika.
- ponašanje na internetu je ogledalo korisnika. Naše ponašanje utječe na ukupnu kvalitetu društvene mreže.
- nemojmo reagirati u ljutnji.
- ako je moguće uključimo dvofaktornu autentifikaciju - (dodatnu prijavu putem koda odaslanog na uređaj po izboru - najčešće naš mobilni uređaj)



TIKTOK

Aplikacija TikTok ima svrhu stvaranja i dijeljenja kratkih videa. Glavni naglasak je na zanimljivim efektima koje se mogu uvrstiti u video, kao i pozadinskoj glazbi koju obično čine popularne pjesme. Najčešći videozapisi koje korisnici objavljuju su plesne tematike, ima tu i komičnih skečeva, a kao i na svakoj društvenoj mreži i izazova.

SAVJET: *Slično kao i poput ostalih društvenih mreža, ima feed (Feed je stream sadržaj kroz koji se možete pomicati) na kojemu se nalaze najpopularniji zapisi, a nakon registracije moguće je i 'lajkati' objave. Račun može biti javan ili privatan, odnosno može se odabrati tko će moći pregledavati sadržaj, a umjetna inteligencija odabire koji će se sadržaj pojavljivati na vašem feedu.*

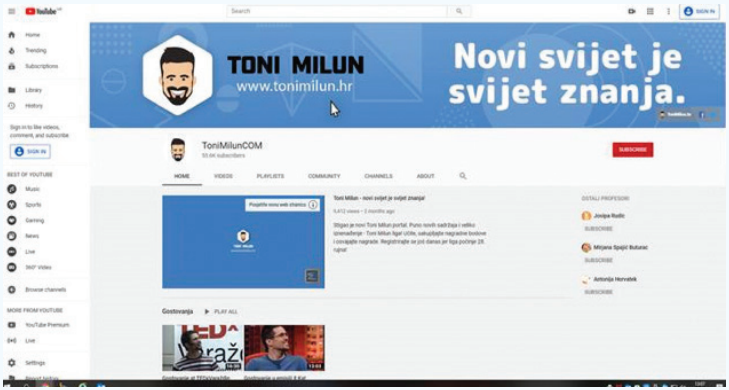
FACEBOOK

Facebook je jedna od najmasovnijih i najpopularnijih društvenih mreža s kojom je većina korisnika već upoznata iako ju djeca najčešće ne koriste. Zahvaljujući Facebook-u možete ostati u kontaktu s osobama koje nisu više u vašoj blizini, koje ne susrećete često – sa rodbinom u inozemstvu, sa prijateljima iz škole. Osim dopisivanja s njima, Facebook možete koristiti kao izvor informacija, za upoznavanje, reklamiranje i povezivanje i socijalizaciju.

SAVJET: *Treba znati da inicijalno Facebook čini listu naših prijatelja koja je javno dostupna. Kako bi to promijenili, potrebno je označiti postavku „Obitelj i odnosi". Tamo su navedeni naši* ***prijatelji****, a klikom na gumb s penkalom pa na „Uredi privatnost", dolazimo do mjesta gdje definiramo tko vidi listu naših prijatelja. Najbolje je odabrati opciju „Prijatelji". Važno je napomenuti da Face, na isti način, nudi kontrolu nad objavom svake pojedine informacije.*
Stoga za sljedeće informacije preporučujemo ograničavanje objave samo na prijatelje:

- *datum rođenja*
- *kontakt informacija (adresa, telefon, elektronička pošta i drugi načini komunikacije)*
- *mjesta rođenja*
- *informacija o zaposlenju*
- *informacija o školovanju*

Više o tome kako zaštiti svoj Face možemo naći na poveznici
http://www.cert.hr/dokumenti/zastitite_privatnost_na_facebooku

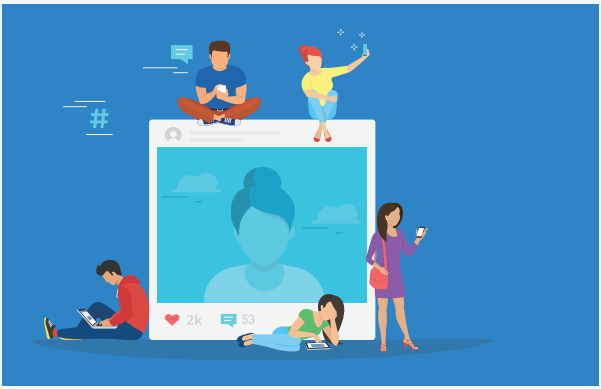


YOUTUBE

YouTube je mrežna usluga za dijeljenje videozapisa gdje se isti mogu postavljati, pregledavati i ocjenjivati te sa sigurnošću možemo reći da je to najbolje mjesto za učenje i stjecanje novih vještina. YouTuberi među mlađom populacijom često imaju sve veći utjecaj od popularnih osoba.

SAVJET: *YouTube – moguće je regulirati postavke uključivanjem „restricted mode – on". Kako bi se to učinilo, potrebno je registrirati se na YouTube – registracija je besplatna. Na dnu prozora će se pojaviti alatna traka i opcija za uključivanje „restricted mode". Kako ni jedan filter nije 100% pouzdan, ipak je potrebno nadzirati dijete dok pretražuje video sadržaj, pogotovo kada je riječ o maloj djeci. Svakako provjerite jeste li prijavljeni u YouTube i je li opcija "restricted mode""uključena prije nego što djetetu prepustite da samo bira video sadržaj.*

- *Ne objavljujmo pod osobnim imenom – možemo izmisliti nadimak za svoj kanal*
- *Imajmo na umu da djeci mlađoj od 13 godina nije dozvoljeno izraditi YouTube račun*
- *Dobro razmislimo hoćemo li objaviti video „Javno" – sami odlučujemo tko će vidjeti naš video.*
- *Možemo drugima ograničiti da dijele naš video, kao i isključiti komentare na svakom videu*
- *Ako vidimo videozapis za koji smatramo da sadrži neprikladan sadržaj možemo ga označiti zastavicom i prijaviti. Vodimo računa o pravu drugih – ukoliko objavljujemo video na kojima je vidljiva druga osoba moramo i od nje zatražiti i dobiti pristanak za objavu*
- *Vodimo računa o glazbi u pozadini – glazba spada pod autorski sadržaj i zaštićena je autorskim pravom – video i glazbu drugih autora možemo koristiti ako je izričito navedeno da je besplatno ili smo zatražili i dobili dopuštenje*
- *Zapamtimo "Bakino pravilo": Upitajmo se je li ono što snimamo ili objavljujemo nešto što bi željeli da vidi naša baka, učiteljica ili roditelj? Ako ne, onda vjerojatno nije dobra ideja objaviti takav video.*



INSTAGRAM

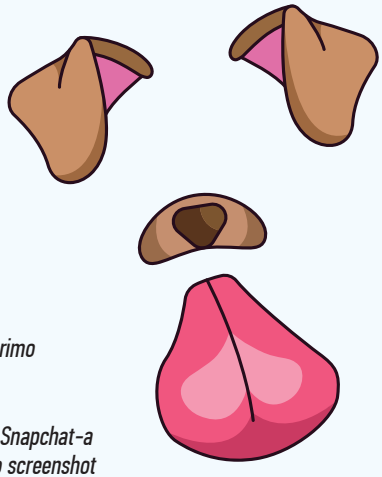
Instagram nam omogućuje dijeliti i komentirati fotografije i video sadržaj, obrađivati fotografije filtrima (filterima) te općenito obilježiti neke trenutke i pratiti što rade drugi. Ovisno o postavkama našeg profila fotografije možemo dijeliti s prijateljima ali i nepoznatim osobama iz cijelog svijeta, koje nas tada mogu slijediti ili otkriti hashtagovima (#). Otvorene profile uglavnom imaju osobe koje žele doprijeti do što više sljedbenika ali otkrivanjem previše informacija možemo se dovesti u opasnost da ih netko zlonamjeran iskoristi.

SAVJET: *Kako zaštiti svoj Instagram profil?*

- *Da zaštitimo privatnost možemo blokirati sljedbenike koje ne poznajemo: na listi sljedbenika odaberemo onog kojeg želimo blokirati i nakon pritiska na tri točkice u gornjem desnom kutu odaberemo opciju blokiranja (Block).*
- *Možemo i zatvoriti profil za nepoznate. Na profilnom prozoru, kliknemo na tri točkice u desnom kutu i pri dnu tog prozora nađemo opciju Privatni račun (Private account) koju uključimo. Tada samo odabrane osobe mogu pristupiti dijeljenim fotografijama i sadržaju.*
- *Uključimo odobravanje označavanja u tuđim fotografijama (tagging). Na taj način moći ćemo odobriti koje tuđe fotografije s nama se mogu pojavljivati na našem profilu.*
- *Sigurnost samog Instagram profila može se povećati uključenjem dvofaktorne autentifikacije, tj. kada se netko želi prijaviti na Instagram na nekom uređaju, tada mora upisati i dodatni kod koji stiže na odabrani broj mobitela naveden u profilu. Nakon pritiska na tri točkice u gornjem desnom kutu pritisnite „Two-Factor Authentication“*

SNAPCHAT

Snapchat je popularna društvena mreža koju koriste tinejdžeri. Snapchat im daje opciju dijeljenja svakodnevnih trenutaka uz zabavne filtere i alate. Za razlika od ostalih društvenih mreža na Snapchatu poruke se nakon čitanja brišu. Da budemo sigurniji i zaštitimo svoju i tuđu privatnost , potrebno je biti oprezan:



SAVJET: *Kako zaštiti svoj Snapchat profil?*

- *Pod opcijama (Settings) pronađimo „See My Location" i odaberimo „My Friends" ili još bolje „Ghost Mode" – (mogućnost ne prikazivanja lokacije)*
- *Obratimo pažnju na obavijesti za vrijeme komunikacije putem Snapchat-a – Snapchat će nam javiti ako je netko s druge strane napravio screenshot Vaše poruke*
- *Pripazite na javno dijeljenje svog Snapchat korisničkog imena čak i ako ste ograničili tko Vas može kontaktirati*
- *Sačuvane poruke koje se nalaze u sjećanjima (Memories) možemo dodatno učiniti sigurnijima tako da ih označimo s „My Eyes Only" što će napraviti posebnu, PIN-om zaštićenu galeriju, tako da ako nekome i pokazujemo prijašnje poruke one koje smo označili s „My Eyes Only" neće biti među njima*

RAČUNALNE IGRE

Nedavne studije pokazuju kako računalne igre pozitivno utječu na razvoj djece, pa se tako navodi da pomažu u logici bržeg rješavanja problema, potiču kreativnost i, povećavaju vizualnu oštrinu i omogućavaju pristup odgojno-obrazovnom sadržaju. Napominjemo međutim da se računalne igre mogu koristiti pod nadzorom odraslih osoba i samo u dijelu slobodnog vremena djeteta/tinejdžera.

SAVJET: *Sadržaj nekih video igara nije namijenjen maloj djeci. U svijetu postoji puno standardiziranih sustava rangiranja računalnih igara. U EU je najpoznatiji PEGI sustav *(Pan European Game Information) koji je osmišljen kako bi pomogao roditeljima/skrbnicima prilikom kupnje videoigara i zaštitio djecu i mlade. Dobna oznaka potvrđuje da je igra prikladna za igrače iznad navedene dobi pa je, primjerice, igra s oznakom PEGI 10 namijenjena djeci od deset godina i starijoj, pri čemu u obzir ne uzima složenost igre, već eventualnu eksplicitnost, neprimjernost i štetnost sadržaja.*
Dogovorite s djetetom vrijeme koje ono smije dnevno provoditi na internetu i igranju video igara.

HAKOM
https://www.hakom.hr, zastita-djece@hakom.hr

Centar za sigurniji Internet
www.csi.hr/ tel. 0800 606 606 – besplatan i anoniman telefon
za pomoć i podršku u slučaju nasilja na internetu

Hrabri telefon
https://djeca.hrabritelefon.hr/ tel:116111, 0800 0800

Poliklinika za zaštitu djece i mladih Grada Zagreba
http://www.poliklinika-djeca.hr/

ANONIMNA PRIJAVA ILEGALNOG SADRŽAJA
www.csi.hr/hotline/

Aplikacija Ministarstva unutarnjih poslova
- namijenjena je svima, ali je posebno prilagođena djeci i omogućuje prijavljivanje sadržaja
na internetu za koji sumnjate da je nezakonit i odnosi se
na različite oblike iskorištavanja ili zlostavljanja djece
https://redbutton.mup.hr/

EU Kids Online
www.hrkids.online

Ova brošura prvenstveno je namijenjena roditeljima i njihovoj djeci u osnovnoj školi,
ali može biti koristan izvor informacija svakomu tko želi više znati
o temi ponašanja i sigurnosti djece na internetu.

Brošura je rezultat suradnje HAKOM-a, Centra za sigurniji internet i Ministarstva znanosti i obrazovanja.

HAKOM | HRVATSKA REGULATORNA AGENCIJA ZA MREŽNE DJELATNOSTI

csi.hr Centar za sigurniji internet

Ministarstvo znanosti i obrazovanja