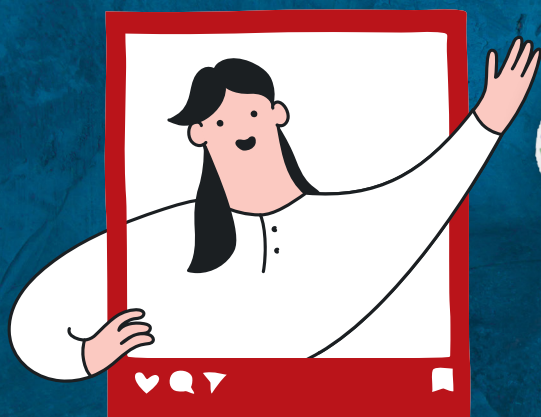


# KAKO SE ZAŠTITITI U SVIJETU INTERNETA I MOBILNIH UREĐAJA



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

# DIGITALNI TRAGOVİ

SU SVE INFORMACIJE  
KOJE OSTAVLJAMO  
SLUŽEĆI SE INTERNETOM

(poruke, objave na društvenim mrežama, videozapisi, fotografije ili crteži, podatci koje upisujemo pri prijavi na mrežnu stranicu).



Danas ne možemo zamisliti život bez interneta i svih mogućnosti koje nam internet pruža. Djeca su pogotovo vezana za internet, on im omogućava brzu komunikaciju, razmjenu ideja, istraživanje, učenje i stvaranje kakvo bez interneta nismo mogli ni zamisliti. No, internet moramo koristiti odgovorno i u tom korištenju moramo poštovati druge ljude. Moderne komunikacijske tehnologije nude gomilu informacija o svemu što bi nas moglo zanimati i omogućavaju komunikaciju, međutim, sloboda koju internet pruža, istovremeno se pretvara u opasnost ako se "mrežom svih mreža" ne znamo služiti na siguran način. Mogućnosti za zlouporabu je mnogo, a najveća opasnost prijeti djeci i maloljetnicima. Promatrajući promjene u učenju, vidimo i promjene u socijalizaciji jer socijalizacija i jest učenje - učenje društvenih vještina, znanja i normi. Mediji i tehnologija značajan su čimbenik socijalizacije baš kao i obitelj, vršnjaci, škola i zajednica. Tehnološke promjene generiraju društvene promjene na neformalnoj i formalnoj, prijateljskoj i poslovnoj razini te uvode nove oblike učenja kao što je e-učenje.

**NAUČIMO DJECU KAKO VIRTUALNI SVIJET RAZLIKOVATI OD STVARNOG SVIJETA TE KAKO ČUVATI PRIVATNOST I PONAŠATI SE U SKLADU S DOBRIM OBIČAJIMA.**

## „EU KIDS ONLINE 2020“<sup>65</sup>

Rezultati istraživanja iz 19 zemalja (EU Kids Online 2020: Survey results from 19 countries), pokazuju rizike i prilike koje internet pruža djeci u Europi. Istraživanje je provedeno u razdoblju od jeseni 2017. do ljeta 2019. u 19 europskih zemalja, a odnosilo se na elektroničko nasilje, gledanje štetnog sadržaja na internetu, zloupotrebu podataka, pretjeranu upotrebu interneta, seksting i upoznavanje nepoznatih osoba na internetu. Istraživači tvrde kako online aktivnosti ne mogu biti uvjerljivo definirane niti kao općenito pozitivne niti kao općenito negativne te kako učinci neke online aktivnosti mogu imati pozitivne posljedice na jedno, a negativne na drugo dijete. Jedan od takvih primjera je susretanje osoba koje su djeca prethodno upozнала samo preko interneta.



- Da većina djece ima **mogućnost pristupanja internetu kad god to želi** ili treba.
- Djeca internetu najčešće pristupaju **putem mobitela/pametnih telefona**.
- Djeca **više vremena provode družeći se i zabavljajući se s prijateljima licem u lice**, nego u online aktivnostima.
- **Količina vremena** koju djeca svakodnevno provode uz internet **raste s dobi djeteta**.
- Djeca na internetu **najčešće slušaju glazbu**.
- Djeca koja imaju i **roditelje** među svojim prijateljima **na Facebooku**, **češće posjećuju društvene mreže**, dopisuju se putem aplikacija te razgovaraju s drugim osobama.

Na što je ukazalo nacionalno istraživanje o medijskim navikama djece i njihovih roditelja te sigurnosti djece na internetu?

61,0%

djece ima profil na društvenoj mreži ili internetskoj stranici za igranje videoigara.

7%

djece u dobi od 9 do 17 godina imalo je iskustvo da se netko ponašao prema njima na povrjeđujući ili neugodan način, dok je 4,5% djece priznalo nasilno ponašanje prema drugima.

1/3

Svako treće dijete svakodnevno ili gotovo svakodnevno nauči nešto novo pretražujući internet.

2/3

Preko 2/3 djece u dobi od 9 do 17 godina na internetu je vidjelo seksualne fotografije ili film gole osobe, a da im nije bila namjera vidjeti ih, dok je gotovo petina njih vidjela takav sadržaj s namjerom.

96%

djece barem ponekad dobiva savjete o sigurnom korištenju interneta od roditelja, nastavnika i prijatelja. Treba istaknuti i da nakon negativnih iskustava na internetu, većina djece u Hrvatskoj najčešće razgovara s roditeljima.

9-17

Djeca u dobi od 9 do 17 godina nedovoljno koriste internet u edukativne svrhe u školi.



U odnosu na djecu iz ostalih 18 država, djeca u Hrvatskoj najrjeđe se suočavaju sa zlouporabom osobnih podataka.

U Hrvatskoj, Španjolskoj, Norveškoj, Poljskoj i Srbiji dječaci češće od djevojčica prijavljuju elektroničko nasilje. Kao i u većini drugih država, i u Hrvatskoj kontakte s nepoznatim osobama na internetu češće ostvaruju starija djeca te češće dječaci od djevojčica.

Rezultati hrvatskog dijela istraživanja ukazuju na potrebu edukacije i podučavanja djece i mladih o njihovoj sigurnosti i mogućim rizicima. Osnovni cilj edukacije je potpora djeci i mladima kako bi što ranije i što uspješnije naučili kontrolirati sadržaje s kojima se susreću na internetu te kako bi se znali snaći u njima potencijalno neugodnim i uznemirujućim situacijama.



## 1.

# ZAŠTITA OSOBNIH PODATAKA NA INTERNETU

Prije registracije na društvenoj mreži važno je pročitati postavke privatnosti.

Zaštita osobnih podataka, u realnom i virtualnom svijetu, postala je ozbiljnija i značajnija. Primjenom Opće uredbe o zaštiti podataka (poznatije kao skraćenica GDPR) nametnute su obveze i pravila svima koji prikupljaju i obrađuju osobne podatke.

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 kako je uvijek sigurnije dati što manje osobnih podataka.



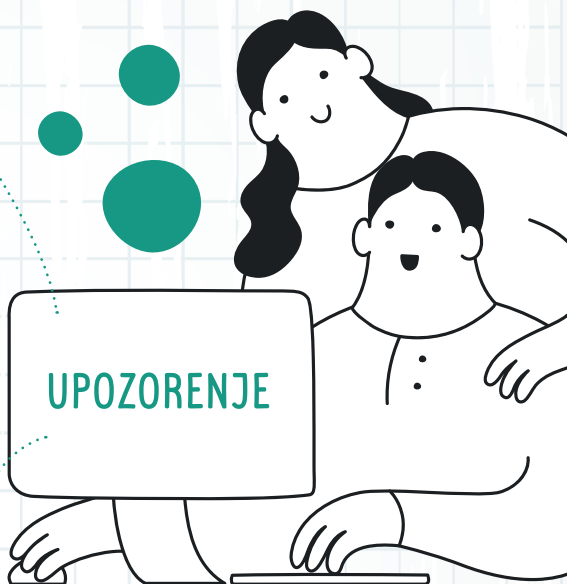
**TREBA IMATI NA UMU KAKO GDPR PROPISUJE DA U SLUČAJU NUĐENJA USLUGA INFORMACIJSKOG DRUŠTVA (NPR. INTERNET TRGOVINE), PRIVOLU ZA OBRADU OSOBNIH PODATAKA DJETETA MLAĐEG OD 16 GODINA MOŽE DATI SAMO RODITELJ ILI SKRBNIK!**



## DJECI, MLADIMA I RODITELJIMA

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

Često objavljujemo sadržaj, ali moramo biti svjesni kako objavljeni sadržaj zauvijek ostaje „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.



## RODITELJIMA

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

## KALKULATOR PRIVATNOSTI



Provjerite potencijalni rizik za vlastitu privatnost prilikom korištenja interneta i davanja osobnih podataka. Uobičajeno se u većini slučajeva traži registracija tijekom koje korisnik mora predati svoje osobne podatke, najčešće adresu e - pošte, 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.

# LAŽNO PREDSTAVLJANJE

Najčešći medij za provedbu ovih prevara su društvene mreže ili specijalizirane web-stranice za online druženje. Napadač nastoji stvoriti iluziju da je riječ o iskrenom i stvarnom odnosu, postupno pridobivajući žrtvino povjerenje, a nakon toga kreće s konkretnijim pokušajima izvlačenja novca. Jedan od primjera je traženje novca za kupnju avionske karte.



# KRAĐA OSOBNIH PODATAKA

Krađa osobnih podataka pojavljuje se kao jedan od rezultata prevare, a u ovu kategoriju ubrajaju se razni tipovi prevara čiji je primarni cilj upravo krađa žrtvinih osobnih podataka. U prvi tip prevara ubrajaju se one koje se zasnivaju na instalaciji zlonamjernog programa (adware, spyware i sl.). Žrtvi se putem poveznice na web-stranici, elektroničke pošte ili društvene mreže ponudi instalacija aplikacije koja napadaču omogućuje pristup žrtvinom računalu.



## 2.

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 svog operatora ili prijaviti primitak takve poruke na adresu elektroničke pošte [nezeljeni.sms@hakom.hr](mailto: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. Također, omogućena je i zabrana 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 računalo 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 kako će od roditelja sakriti 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 takve aplikacije manje su primjerene.

## Upoznajte XOINK

Riječ je o prvoj edukativnoj aplikaciji roditeljske zaštite na svijetu. Xoink je dostupan na Google Playu i iOS-u, a potvrda njene odgojne vrijednosti je i upravo dobivena preporuka Ministarstva znanosti i obrazovanja za upotrebu u osnovnim školama. Aplikacija omogućava da dijete uz korištenje mobitela i uči rješavajući kviz znanja.

Naime, osim što omogućava vremensku kontrolu upotrebe, Xoink ([www.xoink.app](http://www.xoink.app)) djetetu daje i priliku da se dodatno obrazuje. Aplikacija je za djecu od 2 do 18 godina, a nudi četiri modula – Roditelj, Dječji kutak, Starije dijete, Mlađe dijete. Sastoji se od kviz pitanja iz različitih školskih predmeta (geografija, engleski jezik), koja dijete rješava i prema odgovorima može si produljiti vrijeme korištenje, a ujedno i uči i usvaja nova znanja. Potiče na bolju komunikaciju roditelja i djeteta.



## 3.

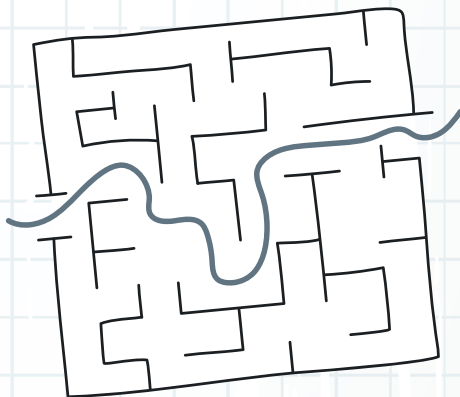
# SIGURNOST I ZAŠTITA NA INTERNETU ZA DJECU, MLADE, RODITELJE I STRUČNJAKE U OBRAZOVNOM PROCESU



Internetska platforma "SINI - Sigurni na internetu" (<https://sini.hr/>) izrađena je s ciljem da se internet učini sigurnijim i boljim mjestom. Edukativnim materijalima i važnim informacijama, na zanimljiv i inovativan način, aplikacija približava područje sigurnosti i zaštite na internetu, a namijenjena je djeci i mladima, roditeljima i stručnjacima, koji rade i surađuju u obrazovnom sustavu. Aplikacija je doprinos stvaranju sigurnijeg okruženja u kojem građani, posebno djeca i mladi, sigurno koriste mobilne uređaje i nove tehnologije. Nastala je kao rezultat suradnje Centra za nestalu i zlostavljaju djecu s Hrvatskom regulatornom agencijom za mrežne djelatnosti (HAKOM-om) i tri hrvatska operatora elektroničkih komunikacijskih usluga, A1 Hrvatska, Telemach Hrvatska i Hrvatskog Telekomu.

Edukativni članci i materijali namijenjeni su djeci, mladima, roditeljima i skrbnicima, a posebno je značajno kako ova platforma omogućava stručnjacima s područja cijele Republike Hrvatske na jednostavan i zanimljiv način stručno usavršavanje kroz formu online webinaru.

Ova mogućnost posebno je značajna stručnjacima u odgojno - obrazovnom procesu u onim dijelovima Hrvatske gdje stručno - edukativne aktivnosti na temu sigurnosti i zaštite djece i mladih na internetu nisu dostupne.



Kako bi mogli pristupiti edukativnom sadržaju putem SINI aplikacije, stručnjaci trebaju proći proces registracije, što će im omogućiti pristup različitim webinarima, a čije je prosječno trajanje od 30 do 60 minuta. Nakon odslušanog webinaru polaže se ispit kako bi se dobio certifikat na temelju kojeg se sudjelovanje prijavljuje nadležnim Komorama. Kako bi se osigurao stručan i kvalitetan sadržaj, koji je dostupan putem internetske aplikacije, kontinuirano se okupljaju stručnjaci iz akademske zajednice i drugih relevantnih institucija i organizacija koji se u svom svakodnevnom radu bave područjem sigurnosti i zaštite djece i mladih na internetu te obrađuju različite teme koje prikazuju u webinarima.

# MEDIJSKA PISMENOST

Medijska pismenost jedna je od ključnih kompetencija za život i rad u digitalnom medijaziranom svijetu koji se konstantno ubrzano razvija i mijenja te za aktivno građanstvo i sudjelovanje u društvenim, ekonomskim, kulturnim i demokratskim procesima. Nove medijske i komunikacijske platforme i tehnološka revolucija doveli su do uslošnjanja medijskoga, komunikacijskoga i društvenoga okružja te potrebe za analitičkim i kritičkim čitanjem brojnih istodobnih izvora informacija. Obitelj je mjesto gdje se odlučuje s kojim će medijima dijete doći u doticaj i kakvu će važnost mediji i s njima povezane aktivnosti imati u djetetovu svakodnevnom životu. **Medijska pismenost uključuje sposobnosti pristupa, analize, vrednovanja i stvaranja medijskih poruka u različitim oblicima. Pristup medijskom sadržaju; važnost kritičkih vještina, odnosno vještina analiziranja i vrednovanja, nužnih za interpretiranje i razumijevanje medijskih sadržaja; i komplementarnost iskustva proizvodnje i stvaranja sadržaja kao alata za učenje kako bi se povećale bitne kritičke sposobnosti.**



# 4.

## APLIKACIJA KOJU SMO RAZVILI SUSRETNICA - što je to?



Osim na internetu povrijediti nekoga (čak i nehotično) možemo i uživo.

Što sve znamo o pristupačnosti usluga i uređaja? Ovdje skrećemo pozornost na još jednu važnu kategoriju korisnika kojom se HAKOM bavi, a to su osobe s invaliditetom. Za njih smo, u suradnji sa FER-om, razvili i aplikaciju **Kviz** koju ti preporučamo pogledati na [www.hakom.hr](http://www.hakom.hr). Naučit ćeš sve o preprekama kojima su izložene osobe s invaliditetom, ali i testirati znanje roditelja o korisničkim pravima.

Baš nas zanima koliko će točnih odgovora prikupiti tvoja obitelj!

Sada skrećemo pozornost na najnoviju aplikaciju **Susretnica**. Često odrasli, a pogotovo djeca, ne znaju kako pravilno pristupiti osobi sa invaliditetom u svakodnevnim situacijama. **Upravo je aplikacija Susretnica osmišljena u svrhu podizanja svijesti o važnosti ispravnog pristupanja osobama s različitim tipovima invaliditeta.** Zato, olakšajmo sebi tako da bolje upoznamo druge. Odaberite između avatara Ane ili Marka i dopustite im da vas povedu putem jače integracije svih članova društva! <http://www.ict-aac.hr/index.php/hr/ict-aac-razvijene-aplikacije/android-aplikacije/ict-aac-susretnica-android>.

## 5.

## METODE ELEKTRONIČKOG NASILJA I UZNEMIRAVANJA

Cyberbullying je korištenje digitalnih medija (kao što su internet i tekstualne poruke) kako bi se druga osoba uznemirila, rastužila ili uplašila i to se ponašanje u većini slučajeva ponavlja.

Neki primjeri cyberbullyinga su: slanje poruka s ciljem da se osoba povrijedi, objavljivanje sramotnih fotografija ili videa na društvenim mrežama i stvaranje glasina na internetu.

Ako tražite informacije kako bi saznali je li vaše dijete žrtva cyberbullyinga, zapitajte se je li ga počinitelj namjerno i u više navrata povrijedio. Ako je odgovor negativan, počinitelj će možda jednostavno morati naučiti kako se ponašati na internetu. Ako je odgovor potvrđan, shvatite situaciju ozbiljno.



Čim vaše dijete počne koristiti internet važno je objasniti mu kakva ponašanja su poželjna i što od njega očekujete.

## NEKI OSNOVNI SAVJETI SU:

### **Komunicirajte na odgovarajući način.**

Koristite odgovarajući jezik za tu priliku i zapamtite da korištenje samo velikih slova znači da vičete, stoga **NEMOJTE TO ČINITI!** ;)

**Nemojte dijeliti informacije kao što su lozinke, vaša kućna adresa, neprikladne slike i tračevi.**

**Poštujte druge. Budite pristojni, a ako se ne slažete s nečim, recite to pristojno.**



Ne pokušavajte prevariti druge, ne zaboravite dati priznanje gdje treba i, iako je lako kopirati tuđi rad, nemojte preuzimati ništa bez dopuštenja.

Podržite one kojima je to potrebno. Ako je netko koga poznajete uznemiravan putem interneta, stanite na njegovu stranu. Željeli biste da ta osoba učini isto za vas.

Prijavite loše ponašanje. Internet je ogromna zajednica i nemoguće je da sve bude savršeno. Koristite alate društvenih mreža za prijavu neprikladnog sadržaja.

Slijedite pravila svoje obitelji. Ako roditelji kažu da izbjegavaš određene web stranice ili da prestaneš slati poruke nakon određenog vremena, poslušaj ih.

Razmislite kako se vi i drugi možete osjećati nakon što nešto objavite. Nije uvijek lako povući ono što ste rekli na internetu, a ono što radite može se dugo snimati.

Razmislite prije nego što objavite,  
pošaljete poruku ili podijelite sadržaj.

## KAKO RODITELJI MOGU POMOĆI?

**1. Smanjite korištenje mobitela/tableta na minimum.**

2. Neka vaša djeca koriste web-lokacije na kojima su poruke za chat unaprijed napisane ili filtrirane prije slanja. Objasnite 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.

**3. 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.**

**4. Objasnite osnove pravilnog ponašanja na internetu (netiquette).**

**5. Dajmo djetetu do znanja da nam se može obratiti svaki put kad na internetu primijeti nešto neprimjereno ili uznemirujuće.**

6. Recite djetetu da ne dijeli svoje lozinke s prijateljima. Jedan oblik zlostavljanja na mreži događa se kada se djeca prijave na tuđu e-poštu ili račun društvene mreže i lažno se predstavljaju.

**7. Objasnite 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.**

## 6.

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 – informiranost je najbolja obrana!

Opasnosti vrebaju putem e – pošte ili poruka za koje se na prvi pogled čini da dolaze od poznate osobe ili tvrtke (Facebook, Ebay, Paypal, Snapchat i dr.). Svrha takvih poruka je da nas potaknu na uošenje 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.

From: Skype Notify <notify@msn.de>  
Date: 20 November 2015 at 00:25  
Subject: Deferred messages pending  
To:

Skype

Deferred message.

[View messages](#)

Yours truly,  
Skype support

© 2015 Skype and/or Microsoft. The Skype name, associated trade marks and logos and the "S" logo are trade marks of Skype or related entities. Skype Communications, S.r.l. 25-28 Via de' Canonici, I-20165 Lombardy

Od: petar <petar.\_\_\_\_@mail.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 mi još vremena da mi naprave novu karticu. Mislio sam te zamoliti da mi posudiš nešto novca koje ću ti vratiti po povratku. Treba mi 1.400 eura da pokrijem troškove. Mogu ti proslijediti detalje o tome kako ti možeš slati novac. Molim te javi mi je li to moguće. Željno iščekujem tvoj odgovor!

S poštovanjem

Petar

## SAVJET:

U SLUČAJU DA PRIMIMO SLIČNU PORUKU NIJE PREPORUČLJIVO KLIKnuti NA POVEZNICU VEĆ U PREGLEDNIKU UNIJETI ADRESU SERVISA, NPR. WWW.FACEBOOK.COM, ULOGIRATI SE I PROVJERITI ČEKAJU LI NAS DOISTA PROPUŠTENE PORUKE

**Ako poruka dolazi od nepoznate osobe nemojmo kliknuti na link ili otvoriti prilog (attachment). Čak i ako je od poznate osobe - budimo oprezni!**

# 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,
- 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

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

# KAKO ZAŠTITITI ADRESU E - POŠTE, 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 lozinke preporuča se poslužiti programom za upravljanje lozinkama. Isto tako, izbjegavajte birati za lozinku osobna obilježja poput mjesta rođenja, imena kućnog ljubimca ili majčinog djevojačkog prezimena. Do tih je podataka vrlo lako doći preko Facebook profila, koji su često otvoreni, ili profila na drugim društvenim mrežama na kojima ljudi objavljuju vrlo osobne podatke ne razmišljajući o tome na koje se sve načine mogu upotrijebiti protiv njih.
- 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 adresu e - pošte od neovlaštenog upada jer šalje dodatni kod na naš mobilni 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!
- **Isključite** bluetooth odmah po prestanku upotrebe jer on predstavlja veliki sigurnosni rizik i lak posao za hakere kada žele doći do podataka na vašem uređaju.
- 3 godine kazne zatvora čeka onoga tko neovlašteno presretne ili snimi nejavni prijenos računalnih podataka, uključujući i elektromagnetsku emisiju računalnog sustava, ili drugome učini dostupnim tako pribavljene podatke.

# PRIJEVARE PUTEM INTERNETA

Internet prijevare se mogu dogoditi i putem aplikacija za komunikaciju poput Vibera, Whatsapp-a ili drugih, kada dobijemo poruku s poveznicom i tekstem 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. Prijevara može biti i telefonskim putem na način da vas prevaranti pokušavaju navesti da otkrijete svoje osobne, financijske podatke ili da im uplatite novčana sredstva. Prevaranti mogu biti i „zainteresirani“ za romantičnu vezu i često koriste društvene medije ili e-poštu za uspostavljanje kontakta.
- 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 „Toster“ zatraži pristup vašim fotografijama i kontaktima, ne bi je trebali preuzeti!

Znaš li da je u okviru završnog rada na FER-u izrađena aplikacija ICT-AAC Lozinka koja se sastoji od kviza, testera i generatora lozinke?

Testirajte je na linku:  
<http://www.ict-aac.hr/index.php/hr/ict-aac-razvijene-aplikacije/web-aplikacije/ict-aac-lozinka>

i ojačajte znanje & digitalnu zaštitu :)



**SAVJET: OSVIJESTITE I DJECU DA NE PREUZIMAJU BILO KAKVE APLIKACIJE, ODNOSNO DA IH ZAJEDNIČKI PREGLEDATE I PROKOMENTIRATE PRIJE SAME INSTALACIJE I KORIŠTENJA.**

## 7.

## 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:

Opća pravila sigurnijeg korištenja društvenih mreža i programa za razmjenu poruka:

- što je nezakonito u stvarnom životu nezakonito je i na internetu
- ne ostavljajmo privatne informacije, bilo na fotografijama bilo u opisima
- ne otkrivajmo svoju lokaciju ako nije potrebno
- 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. #Ulica13
- ne dijelimo nasilne ili nepristojne fotografije. Pripazimo što šaljemo u svijet. Ne samo što stvaramo sliku o sebi već utječemo i na druge
- ne sudjelujemo u nasilju putem interneta. Ne omalovažavamo 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
- poštujujmo 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

Tik Tok je novija društvena mreža, odnosno aplikacija, koju možemo usporediti s YouTube, Instagram ili Facebook aplikacijama.

Ciljna starosna grupa ovoj aplikaciji su osobe u dobi između 16 i 24 godine, međutim koriste je već djeca od 8 godina pa na dalje. Aplikaciju mogu samostalno koristiti djeca već od navršениh 13 godina, ali ako to učine ranije profil im se briše.

Tik Tok je aplikacija koja svojim korisnicima daje mogućnost kreiranja kratkih video snimki. Riječ je o društvenoj aplikaciji, pa će jednom napravljen video biti dostupan za gledanje vlasniku video materijala, ali i drugim osobama s kojima je povezan. Aplikacija je prisutna još od 2016., no tek je u zadnjem periodu doživjela veliku svjetsku popularnost. Najčešći videozapisi koje korisnici objavljuju su plesne tematike, ima tu i komičnih skečeva, a kao i na svakoj društvenoj mreži i izazova.

Ako vaše mlađe dijete želi koristiti aplikaciju, postoji odjeljak aplikacije za djecu mlađu od 13 godina koji uključuje dodatne opcije sigurnosti i privatnosti. Djeca mogu vidjeti samo uređene, čiste videozapise i ne smiju komentirati, pretraživati ili objavljivati vlastite videozapise. Međutim, to ga čini neprivačnim za većinu djece, a zaobilazanje sigurnosnih uvjeta zahtijeva samo unošenje lažnog datuma rođenja, pa nije savršen.

Bez obzira što mnogi misle da je to platforma za kreativno izražavanje, iskazivanje talenata i zabavljanje, 90% videozapisa na TikTok-u je neprikladno, pa su roditelji zabrinuti trebaju li izbrisati račun svoje djece na Tik Tok-u ili ne. Ono što je karakteristično za ovu platformu je da na njoj korisnici mogu vrlo brzo "steći slavu".

Postoji ogroman poticaj da se postane poznat, uključujući TikTok kuće u kojima grupe mladih kreatora žive i snimaju videozapise - i ubiru velike novce i sponzorstva. Djecu koja gledaju ovaj primjer može se nagovoriti da učine ili podijele stvari koje inače ne bi radili kako bi privukli veću publiku.

Postoji široka zabrinutost zbog širenja potencijalno štetnih online izazova posebice na ovoj platformi koje su utjecale na ozljeđivanje i smrtnost djece.

Kroz odrastanje nikad nije nedostajalo izazova, ali čini se da današnja djeca žive u posebno teškom razdoblju. S obzirom da je globalna pandemija koronavirusa usmjerila dječje živote još više prema internetu, sa sigurnošću se može reći da je potreba za lako dostupnim tehnološkim alatima, koje djeca mogu koristiti privatno i sigurno, za mentalno zdravlje kritičnija nego ikad.

**Također mogu postati opsjednuti lajkovima i virtualnim odobravanjem, što nije zdravo za njihovu emocionalnu dobrobit.**

**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 web mjesto na društvenim mrežama na kojem korisnici mogu objavljivati komentare, dijeliti fotografije i objavljivati veze do vijesti ili drugog zanimljivog sadržaja na webu, razgovarati uživo i gledati videozapise u kratkom obliku i tu mrežu djeca najmanje koriste. Možete čak i naručiti hranu na Facebooku, ako je to ono što želite raditi. Dijeljeni sadržaj može biti javno dostupan ili se može podijeliti samo s odabranom grupom prijatelja ili obitelji ili s jednom osobom.

Facebook pruža prilagodljiv skup kontrola privatnosti, tako da korisnici mogu zaštititi svoje podatke od navale na treće osobe.

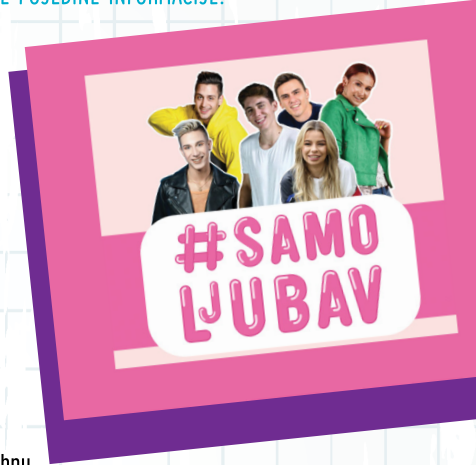
**SAVJET: TREBA ZNATI DA INICIJALNO FACEBOOK ČINI LISTU NAŠIH PRIJATELJA KOJA JE JAVNO DOSTUPNA. KAKO BI TO PROMIJENILI, POTREBNO JE OZNAČITI POSTAVKU „OBITELJ I ODNOSI“. TAMO SU NAVEDENI NAŠI PRIJATELJI, A KLIKOM NA GUMB S PENKALOM PA NA „UREDI PRIVATNOST“, DOLAZIMO DO MJESTA GDJE DEFINIRAMO TKO VIDI LISTU NAŠIH PRIJATELJA. NAJBOLJE JE ODABRATI OPCIJU „PRIJATELJI“. VAŽNO JE NAPOMENUTI DA FACE, NA ISTI NAČIN, NUDI KONTROLU NAD OBJAVOM SVAKE POJEDINE INFORMACIJE.**

Više o tome kako zaštititi svoj Face možemo naći na poveznici [http://www.cert.hr/dokumenti/zastitite\\_privatnost\\_na\\_facebooku](http://www.cert.hr/dokumenti/zastitite_privatnost_na_facebooku)

## YOUTUBE

YouTube je mrežna usluga za razmjenu videopisa gdje se isti mogu postavljati, pregledavati i ocjenjivati te sa sigurnošću možemo reći da je to najbolje mjesto za učenje i stjecanje novih vještina. Za postavljanje sadržaja potrebna je registracija, dok za pregledavanje nije, osim sadržaja koji nije primjeren za osobe mlađe od 18 godina.

Youtuberi među mlađom populacijom često imaju sve veći utjecaj kao popularne osobe, a neki više vjeruju virtualnim uzorima nego obitelji i prijateljima. Kvalitetni i popularni Youtuberi mogu pozitivno utjecati na djecu, ovisno o sadržajima kakve stvaraju i objavljuju. Posebnu pažnju treba posvetiti aplikaciji YouTube Kids, gdje svatko može stvoriti YouTube kanale bez dodatnih provjera, a sadržaj je generiran od strane korisnika.



**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 KAD 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 video 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  
Opcija „Privatno“ omogućava odabir ljudi koji mogu vidjeti video, a opcija „Nenavedeno“ da video mogu vidjeti samo oni kojima se link pošalje
- Možemo drugima ograničiti da dijele naš video, kao i isključiti komentare na svakom videu
- Ako vidimo videopis 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

Znate li:

- da je 23. travnja 2005. postavljen prvi video naziva „Me at the ZOO“, autora Jaweda Karima koji je jedan od osnivača te mrežne usluge? <https://youtu.be/jNQXAC9IVRw>
- da je Matej Lončarić stručnjak za YouTube sadržaj u Republici Hrvatskoj i pokretač projekta i kanala JoomBoos (kanal koji okuplja najpoznatije YouTubere u Hrvatskoj i regiji)
- da je HAKOM sudionik kampanje #SAMOLJUBAV Anti Cyberbullying kampanje preko JoomBoos kanala
- da inicijativa Boli Me. pruža podršku mentalnom zdravlju mladih i otvara Muzej empatije...
- Svakako preporučamo posjetu ovoj oazi mira i jednakosti na: <https://www.bolime.hr/>, a možete ih zapratiti i na: <https://youtu.be/6dGGqWRpxDQ>

## INSTAGRAM

Instagram je jedna od najpopularnijih društvenih platformi za razmjenu slika. Tinejdžeri vole Instagram iz više razloga, ali što je najvažnije, tu su njihovi prijatelji. Također mogu pratiti omiljene slavne osobe, ostale osobe koje su im zanimljive i, naravno, održavati vlastiti profil (ili profile) kojim svojim prijateljima – a ponekad i svijetu predstavljaju sliku o sebi.



Ovisno o tome koga pratite ili što tražite, možete pronaći i puno sadržaja za odrasle. A komentari na objave mogu biti neprimjereni, pogotovo ako je račun javan. Djeca ponekad osjećaju kako moraju održavati savršen profil, pa prestano skeniraju postove u potrazi za lajkovima i brišu one koji ne zadovoljavaju njihove kriterije. Ipak, uz neke smjernice oko postavki, ograničenja upotrebe i neprekidne razgovore o sadržaju i komentarima, Instagram može biti korisno mjesto za djecu koje im omogućava da se povežu i budu kreativni. Vrste sadržaja koje će djeca vidjeti uglavnom ovise o tome koga slijede: ako prate samo prijatelje i ne traže ništa, možda će vidjeti samo slike svojih prijatelja kako se zabavljaju. Ali djeca rijetko ograničavaju svoje feedove na ljude koje poznaju, pa će vjerojatno vidjeti sadržaj za odrasle. Ako prate poznate osobe, vjerojatno će vidjeti i marketinške oglase. Koristi li se pozitivno, Instagram je mjesto na koje djeca odlaze da bi se povezala s prijateljima. Tinejdžeri ga također koriste za kreativnost, objavljivanje umjetnina, poezije i videozapisa, kako bi pokazali svoje talente. Ako se koristi uravnoteženo s drugim aktivnostima i sa svrhom, djeca se mogu osjećati zadovoljno i prihvaćeno, primjerice, ako dobivaju pozitivne komentare na svoje umjetničke fotografije, slike, pjesme i slično.

## SAVJET: KAKO ZAŠTITI SVOJ INSTAGRAM PROFIL?

1. Kako bi zaštitili 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).
2. 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.
3. Uključimo odobravanje označavanja u tuđim fotografijama (tagging). Na taj način moći ćemo odobriti koje se tuđe fotografije na kojima smo označeni mogu pojavljivati na našem profilu.
4. Sigurnost samog Instagram profila može se povećati uključanjem 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 za razmjenu poruka koja omogućava korisnicima razmjenu slika i videozapisa (zvanih snaps) koji bi trebali nestati nakon što ih pogledaju. Oglašava se kao „nova vrsta fotoaparata“ jer je osnovna funkcija snimanje slike ili videozapisa, dodavanje filtara, leća ili drugih efekata i dijeljenje s prijateljima. Na Snapchatu fotografije, a ne tekst, obično započinju komunikaciju. Jednom kada prilagodite svoj snimak, možete ga poslati bilo kome s popisa prijatelja ili dodati u svoju priču, što je zapis dana koji vaši prijatelji mogu gledati 24 sata. Uz pojedinačno slanje poruka, Snapchat nudi i grupno slanje SMS-ova i grupne priče kojima svi u grupi mogu pridonijeti. Možete izbrisati tekstualne poruke koje šaljete, iako će u grupnom chatu drugi ljudi vidjeti da ste nešto izbrisali.



Nestaju li poruke zaista na Snapchatu? Ovisi. Ako postavite vremensko ograničenje na trenutak, ono će nestati nakon što ga pregledate. No, primatelji mogu snimiti snimku zaslona slike koristeći svoje telefone ili aplikaciju za snimanje zaslona treće strane. Snimanje zaslona telefona obavijestit će pošiljatelja da je slika snimljena. No, aplikacije trećih strana ne pokreću obavijest. Iz tih razloga najbolje je da tinejdžeri shvate kako ništa što se radi na mreži stvarno nije privremeno. Prije slanja neugodnog snimka sebe ili nekoga drugog, važno je imati na umu kako bi ta snimka mogla kružiti školom već sutra ujutro. Budući je tako lako pronaći prijatelje na Snapchatu (ovisno o vašim postavkama) ili razmijeniti kodove, tinejdžeri mogu na kraju biti s virtualnim strancima na popisu prijatelja. Iz različitih razloga to može biti rizično, pa je najbolje razgovarati sa svojim tinejdžerima o tome kada je sigurno dodati ljude.

## SAVJET: KAKO ZAŠTITI SVOJ SNAPCHAT PROFIL?

1. Pod opcijama (Settings) pronađimo „See My Location“ i odaberimo „My Friends“ ili još bolje „Ghost Mode“ – (moćnost ne prikazivanja lokacije)
2. Obratimo pažnju na obavijesti za vrijeme komunikacije putem Snapchat-a – Snapchat će nam javiti ako je netko s druge strane napravio screenshot Vaše poruke
3. Pripazite na javno dijeljenje svog Snapchat korisničkog imena čak i ako ste ograničili tko Vas može kontaktirati
4. 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

# 8.

## VIDEOIGRE

Videoigre omogućuju istraživanje i kreativno izražavanje – umjesto nametanja krute strukture – jako su dobre za učenje jer potiču kritičko razmišljanje, rješavanje problema i logičko zaključivanje (učenje kako stvari rade zajedno). Dogovorite s djetetom vrijeme koje ono smije dnevno provoditi na internetu i igranju videoigara.

Za provjeru prikladnosti sadržaja videoigara koriste se ESRB i PEGI sustavi koji kategoriziraju videoigre prema uzrastu djece i prema vrsti sadržaja koji igra sadrži. Prije kupnje igre, provjerite PEGI ili ESRB oznaku.

### ROBLOX

Videoigra unutar koje možete igrati igre i mape koje su dizajnirali drugi korisnici i stvarati i dijeliti vlastite igre koristeći Robloxov vlastiti alat za razvoj igara. Jednom kada se prijavite, možete igrati beskonačan broj igara, graditi i dijeliti kreacije i razgovarati s drugim korisnicima – i sve besplatno. Ako vaša djeca igraju Roblox, trebat će im Robux i vjerojatno će se htjeti pretplatiti na Builders Club, koji pruža dodatne značajke uz članarinu. Roblox potiče korisnike na interakciju putem svoje funkcije Chat & Party. Sav je chat filtriran, što znači da je neprimjeren jezik zamijenjen hashtagovim simbolima. Razgovori s djecom mlađom od 13 godina filtrirani su više. Roblox također zapošljava moderatore koji paze na neprikladan jezik i sadržaj. Kao i u bilo kojoj drugoj videoigri, benefita ima mnogo, ali s obzirom da se radi o online igri, uvijek postoji opasnost od zlonamjernih ljudi.

### MINECRAFT

Minecraft je avanturistička videoigra. Stil se naziva “sandbox” (pješčanik) jer pruža kreativni krajolik bez fiksnog cilja i beskrajnih je mogućnosti. Njegov kockasti dizajn također je prilično dječji: glave likova su četvrtaste, boje se pojavljuju u komadima, pa čak i drveće izgleda kao da je uzgojeno u Lego laboratoriju. Kao i svako igralište, Minecraft ne dolazi s uputama, a relativno ga je jednostavno podići i igrati. Igru učite istraživanjem, eksperimentiranjem, gledanjem YouTube videozapisa i čitanjem drugog sadržaja stvorenog od obožavatelja.

Minecraft je vrlo siguran za djecu. Primjerice, u kreativnom načinu za jednog igrača nema interakcije s drugima i sukoba. No, s vremenom se većina djece želi igrati s drugima, a igranje više igrača donosi određene rizike. Iako su Minecraft zajednice uglavnom pozitivne, a moderatori poslužitelja odgovorni su za održavanje reda, djeca se mogu izložiti psovkama, maltretiranju, pa čak i govoru mržnje. Ni Minecraft nije imun na grabežljivce, a budući da ljubitelja igre ima u svim dobnim skupinama, uključujući odrasle, okruženja koja stvaraju igrači mogu sadržavati bitke, seksualne scenarije i drugi sadržaj primjereniji za odraslu publiku. Usredotočenost Minecrafta na izgradnju može ojačati koncepte geometrije, jer jača logičke vještine, kreativnost, pa čak i suradnju igrača, ali obrazovna vrijednost bilo kojeg medija ima puno veze s onim tko vodi učenje.

## FORTNITE

Fortnite je videoigra koja uzima elemente iz „sandbox“ igara i dodaje brzu akciju pucnjave iz trećeg lica.

Postoje dva načina igre: samostalna verzija pod nazivom Save the World i izuzetno popularna verzija za više igrača pod nazivom Battle Royale. Za neke roditelje crtani, beskrvni stil radnje u Fortniteu čini nasilje manje problematičnim od agresivnih krvarenja u drugim popularnim pucačkim igrama. Ali s obzirom kako se radi o online igri, opasnost se može pojaviti u chatu u igri - posebno u Battle Royaleu - mogla bi izložiti mlađe igrače uvredljivim riječima ili neprimjerenim sadržajima slučajnih stranaca.

## STVARAJU LI VIDEOIGRE OVISNOST?

Potpuna zabrana videoigara može onemogućiti djetetu dijeljenje iskustava s vršnjacima, dok igranje bez granica može imati još štetnije posljedice.

Svjetska zdravstvena organizacija (WHO) identificirala je stanje koje se naziva poremećaj internetskih igara (IGD), a koje bi, prema njihovoj ocjeni, moglo biti vrsta ovisnosti, premda je potrebno još istraživanja. Ali IGD je rijedak i često može biti povezan s drugim stanjima kao što su depresija i ADHD, jer videoigre ne stvaraju ovisnost same po sebi. Iluzija uspjeha u virtualnom svijetu čini igre privlačnima, ali samo iz razloga što neki tinejdžeri igre ne koriste kao zabavu, već im ona služi kao bijeg od pravih problema i stvarnosti s kojom se svakodnevno suočavaju (disfunkcionalne obitelji, vršnjačko nasilje, osjećaj neprihvaćenosti).



## GOOGLE PLAY ZAMKE

Google Play Googleova je mrežna trgovina za aplikacije, glazbu, filmove i ostale digitalne sadržaje iz 2008.

Za korištenje Google Play-a potrebno je imati uređaj i Google adresu e - pošte, a po prijavi dostupan sadržaj moguće je kupovati kreditnom/debitnom karticom.

Također zahvaljujući suradnji Google-a i naših operatera, željeni sadržaj možete plaćati i putem svog korisničkog računa i na taj način zaobići unos podataka o kreditnoj/debitnoj kartici.

Po uspješno obavljenoj transakciji zaprimiti ćete potvrdu na Google adresu e - pošte.

U cilju onemogućavanja neovlaštenih transakcija (najčešće od strane djece) jako je bitno **UKLJUČITI PROVJERU AUTENTIČNOSTI!**



Za postavljanje provjere autentičnosti otvori Google Play/ meni/ "Postavke"/ "Zahtijevaj provjeru autentičnosti za kupnju"

Za igre i/li aplikacije moguće je tražiti povrat unutar 2 sata od kupnje.

Kako bi zatražili povrat trebate otvoriti Google Play aplikaciju (Trgovina Play).

1. Odaberite Meni - Račun - Povijest narudžbi.
2. U popisu kupljenih sadržaja pronađite igru ili aplikaciju koju želite vratiti.
3. Odaberite "Povrat" i aplikacija će se sama ukloniti s vašeg uređaja.

Maksimalni iznos pojedine transakcije za kupovine u Google Play trgovini iznosi 375 kn. Ukupni mjesečni iznos koji možete potrošiti u Google Play trgovini iznosi 500 kn.

Zna li da se može postaviti iznos mjesečnog proračuna koji se ne želi probiti, a sustav će automatski obavještavati kada mu se približite?

U postavkama možete uključiti „Roditeljski nadzor“ pa nakon unosa PIN-a biraš razinu zaštite i ograničavaš skidanje sadržaja.

Super korisna je i opcija Google Family Linka koja se preuzima na uređaj i sugerira koje su aplikacije prikladne za dob djeteta, nadzire online aktivnost, ograničava vrijeme korištenja uređaja, omogućava daljinsko zaključavanje djetetovog uređaja, određuje njegovu lokaciju i još štošta. Za više informacija, link je u nastavku: <https://families.google.com/intl/hr/familylink>

# 5G KAO NAŠA SADAŠNJOST

**Digitalne vještine biti će još važnije, a razumijevanje tehnološkog napretka nužno. Unatoč čarima virtualnog svijeta, nemojte zaboraviti ljepote stvarnog.**

Kao i do sada, i s 5G tehnologijom vrijede sva pravila vezana uz sigurnu uporabu internetskih aplikacija kojih se treba pridržavati. A nove aplikacije i nove mogućnosti donijet će i nova pravila kako bismo i dalje sigurno plovili internetom. Također, vrijeme provedeno s pametnim uređajima bez obzira koriste li oni 5G ili 4G tehnologiju, treba ipak biti razumnog trajanja. Najbitnije karakteristike nove 5G tehnologije su velike brzine, visoka razina pouzdanosti te malo kašnjenje signala. To znači da će se aplikacije pokretati brže, da će zvuk i slika biti kvalitetniji i da će se razvijati nove aplikacije u svim područjima života.

## ZNAŠ LI DA 5G OMOGUĆUJE DA:

- svi građani RH imaju jednako kvalitetan pristup internetu
- gradovi postanu „pametni“ (regulirati će tako razinu električne energije, popunjenost parkinga, potrebu za odvozom smeća)
- automobili međusobno „pričaju“ i dijele informacije kojima će se optimizirati promet i spriječiti nesreće
- posao i videoigre budu u „oblaku“ (programu, dokumentu može se pristupiti s većeg broja uređaja, u bilo koje vrijeme i s različitih lokacija uz internetsku vezu)
- videoigre budu u „realnom“ vremenu
- unaprijede rješenja u industriji, poljoprivredi, području javne sigurnosti, financijskih usluga, zdravstvu te energetici
- se još snažnije razvije umjetna inteligencija (AI). Za one željne znanja na linku <https://www.elementsofai.com/hr/> nalazi se tečaj o osnovama AI. On je besplatan, traje 6 tjedana, dobiva se potvrda i čak 2 ECTS boda!

Razvoj tehnologije omogućuje pružanje novih usluga i aplikacija čiji korisnici nisu više samo ljudi nego i uređaji koji će unositi i razmjenjivati veliku količinu osjetljivih podataka na mreži, što povećava potrebu zaštite računalne "imovine" i kibernetičke sigurnosti - cybersecurity.

**I za kraj, naša preporuka za gledanje s obitelji:**



## HAKOM

<https://www.hakom.hr>, [zastita-djece@hakom.hr](mailto:zastita-djece@hakom.hr)

### Centar za sigurniji Internet

[www.csi.hr](http://www.csi.hr)/ tel. 0800 606 606 – besplatan i anonimni 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/](http://www.csi.hr/hotline/)

### [redbutton.gov.hr](http://redbutton.gov.hr) 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

### EU Kids Online

[www.hrkids.online](http://www.hrkids.online)

Prati JoomBoos anti-cyberbullying kampanju, pridruži nam se u borbi protiv online i svih drugih oblika nasilja i pokaži da ti podržavaš #SAMOLJUBAV!

### Sveučilište u Zagrebu Fakultet elektrotehnike i računarstva,

Laboratorij za asistivne tehnologije i potpomognutu komunikaciju, <http://lab.ict-aac.hr/>

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.



HRVATSKA REGULATORNA AGENCIJA  
ZA MREŽNE DJELATNOSTI



Ministarstvo  
znanosti i  
obrazovanja