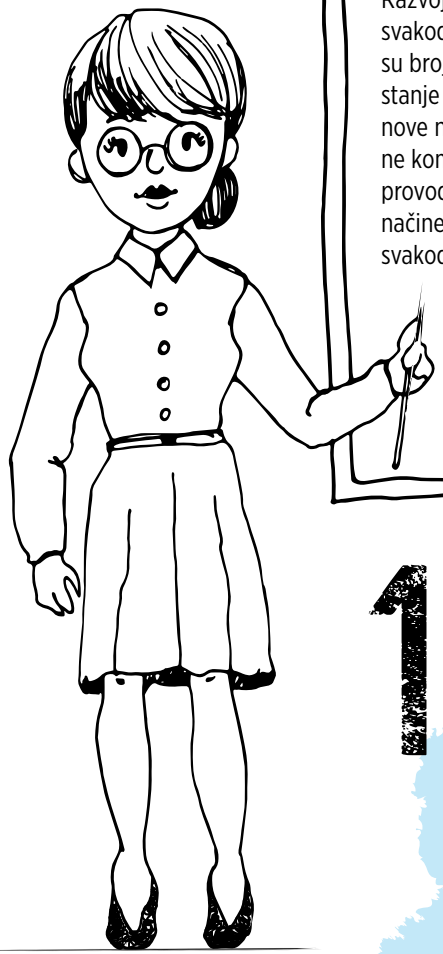
HAKOM

KAKO ZAŠTITITI DIJETE

u svijetu interneta, mrežnih tehnologija i mobilnih telefona



Razvoj modernih tehnologija i pojava interneta kao svakodnevnog medija u ljudskim životima povećali su broj faktora koji izravno utječu na razvoj i odrastanje djece i mladih. Suvremeno društvo ima neke nove načine pristupa informacijama, neke nove načine komuniciranja s prijateljima i obitelji, nove načine provođenja slobodnog vremena, pa čak i nove načine kupovine, druženja, obrazovanja, obavljanja svakodnevnih zadataka. Sve navedeno u osjetljivom razdoblju rasta i razvoja u kojem se nalaze djeca i mladi oblikuje mišljenja, stavove i vrijednosti na drugačiji način nego prije pojave „digitalnog društva".

1. ISTRAŽIVANJE EU KIDS ONLINE

Tijekom listopada i studenoga 2017. provedeno je **najveće i najsveobuhvatnije nacionalno komparativno istraživanje** o medijskim navikama djece i njihovih roditelja te sigurnosti djece na internetu. Istraživanje je provedeno u sklopu projekta ˝EU Kids Online˝ i obuhvatilo je **1017 djece u dobi od devet do 17 godina i njihove roditelje.**

- Svako četvrto dijete u dobi od devet do 14 godina te svako treće dijete u dobi od 15 do 17 godina u potpunosti ili uglavnom zabrinuto je za svoju privatnost na internetu
- Svako peto dijete u dobi od devet do 17 godina u potpunosti ili uglavnom **ne zna promijeniti postavke privatnosti, npr. na društvenim mrežama**
- Gotovo svako treće dijete u dobi od devet do 17 godina u posljednjih godinu dana komuniciralo je na internetu s osobama koje nije upoznalo uživo

- Više od desetine djece u dobi od devet do 17 godina u posljednjih godinu dana susrelo se uživo s osobom koju je upoznalo na internetu. **Nemojte ići sami na susrete s nepoznatnim osobama koje ste upoznali online**
- U proteklih godinu dana više od pola djece u dobi od devet do 17 godina primilo je povrjeđujuću ili neprimjerenu poruku
- Gotovo dvije trećine djece u dobi od devet do 17 godina na internetu je u proteklih godinu dana vidjelo seksualne fotografije ili film gole osobe, a da im nije bila namjera vidjeti ih
- Svako deseto dijete u dobi od 15 do 17 godina **prihvaća sve zahtjeve za prijateljstvom drugih ljudi na društvenim mrežama**

IZVOR: HRKIDS.ONLINE

Istraživanje je, osim toga, pokazalo da je tek svako deseto dijete tražilo pomoć druge osobe kada je primilo povrjeđujuću ili neprimjerenu poruku. Roditelji, razgovarajte s djecom o njihovim iskustvima korištenja medija i društvenih mreža!

Dragi mladi, tražite pomoć svojih roditelja kada vas uznemiri nešto u virtualnom svijetu.

2. KORISNI SAVJETI ZA RODITELJE

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, www.hakom.hr

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 koje su namijenjene djeci (50,00 kn).

Svaki operator koji pruža i usluge televizije, omogućava roditeljsku zaštitu koja se može aktivirati po potrebi i željama korisnika.

3. VRŠNJAČKO NASILJE PUTEM INTERNETA

Problem koji zaokuplja pažnju roditelja, nastavnika i stručnjaka koji odgajaju i obrazuju djecu i mlade, a o kojem se u posljednje vrijeme puno govori je vršnjačko nasilje putem interneta. Zabrinjava jer ga je teško kontrolirati i spriječiti, a ostavlja ozbiljne posljedice na žrtve.

Vršnjačko nasilje poznato nam je oduvijek, s njim smo se naučili suočavati i na njega reagirati, ali pojava interneta dala mu je novu dimenziju i nove karakteristike. I dalje su roditelji, ali i stručnjaci, povremeno zbunjeni i ne znaju kako postupiti u slučaju vršnjačkog nasilja putem interneta. Osim zajedničkih karakteristika koje imaju „tradicionalno" i „moderno" vršnjačko nasilje poput agresivnosti, namjere da se nekoga povrijedi te nemogućnosti žrtve da se obrani, „moderno" vršnjačko nasilje 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, videozapisi i agresija ostaju na internetu i svima su dostupni, neovisno o tome gdje se nalazili. Nadalje, počinitelj nasilja na internetu ima veći osjećaj anonimnosti nego što je to slučaj kod nasilja u stvarnom svijetu. Iako žrtva najčešće zna tko je počinitelj, on u velikom broju slučajeva izbjegne sankcije za svoje ponašanje. S druge strane, počinitelj za vrijeme nasilnog ponašanja putem interneta ne može vidjeti reakcije svoje žrtve, zbog čega njegovo ponašanje može postati još agresivnije i bezobzirnije.

U KONAČNICI, ČINI SE DA DRUŠTVO JOŠ NE SMATRA DA JE NASILJE PUTEM INTERNETA OBLIK NASILJA KOJI MOŽE IMATI OZBILJNE POSLJEDICE TE NERIJETKO MOŽEMO ČUTI DA SE TO NIJE DOGODILO U „STVARNOM SVIJETU" TE DA SU ŽRTVE SAMO PREOSJETLJIVE NA SITUACIJU KOJA UOPĆE NIJE TAKO OZBILJNA. NAŽALOST, OZBILJNOST SITUACIJE SHVATIMO TEK KADA JE ŠTETA VEĆ POČINJENA.

Koji su znakovi izloženosti nasilju putem interneta?

ŽRTVE VRŠNJAČKOG NASILJA PUTEM INTERNETA NAJČEŠĆE IMAJU SLJEDEĆE SIMPTOME:

IZBJEGAVANJE UOBIČAJENIH AKTIVNOSTI, ŠKOLE, PRIJATELJA I GRUPNIH OKUPLJANJA

NESANICA I GUBITAK APETITA

NAGLE PROMJENE RASPOLOŽENJA

IZBJEGAVANJE UOBIČAJENIH AKTIVNOSTI, ŠKOLE, PRIJATELJA I GRUPNIH OKUPLJANJA

PRESTANAK KORIŠTENJA MOBITELA, RAČUNALA, INTERNETA

POVUČENOST TE IZBJEGAVANJE RAZGOVORA O SVOJIM AKTIVNOSTIMA NA INTERNETU I DRUŠTVENIM MREŽAMA

Kako roditelji mogu pomoći?

1. 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. 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 poštovati i prema njima se primjereno ponašati te od njih očekivati isto.

2. BUDIMO UPOZNATI S PONAŠANJEM SVOG DJETETA NA INTERNETU. Kao što želimo znati s kim naše dijete provodi vrijeme u stvarnom svijetu, trebali bismo znati i **s kim provodi vrijeme u virtualnom svijetu.**

3. 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 odredite 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.

4. OPASNOSTI NA INTERNETU

OPASNOSTI NA INTERNETU SU VELIKE I POSTOJI ČITAVA VOJSKA LJUDI ČIJI JE JEDINI CILJ NAĆI NAČIN KAKO IZIGRATI NAŠE POVJERENJE, PODATKE I RAČUNALO ZA ISPUNJENJE SVOJIH CILJEVA.

Kako bi pristupili našim podacima i računalima, kriminalci se koriste malicioznim (zlonamjernim, štetnim) programima kojima zaobilaze zaštitu naših računala. U ovom trenutku, dnevno se otkrije oko **3000 novih malicioznih programa,** 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.

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 nas netko na internetu može pokušati prevariti?

Putem elektroničke pošte, slanjem poruka za koje se na prvi pogled čini da dolaze od neke poznate tvrtke (Facebook, eBay, PayPal, Snapchat i sl.) ili sličnim načinima. Svrha takvih poruka je da nas potaknu na unošenje naših pristupnih podataka u aplikaciju čime kriminalcima dajemo pristup svojim podacima. A jednom kada imaju podatke o nama, oni mogu načiniti značajnu štetu, primjerice **uzeti kredit u naše ime, obaviti kupnju 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!

Internetskim tražilicama poput Googlea ili Binga dostupno je manje od 10% cijelog interneta

PRIMJER:

http://privatnost.hakom.hr/category_hr.php

Kako prepoznati lažnu poruku?

NEKI OD ZNAKOVA PO KOJIMA SE MOŽE PREPOZNATI DA JE PORUKA LAŽNA:

NE OBRAĆA SE OSOBNO NAMA, nego počinje nekim općenitim pozdravom npr. „Hi there“, ili „Hey you“ ili „Bok!˝

IME SERVISA I ADRESA S KOJE PIŠE DA JE PORUKA DOŠLA NISU ISTI
U donjem primjeru poruka izgleda kao da je došla od Skypea, no Skype ima domenu @skype.com, a ova poruka je došla sa (s) @pmw.de

PORUKA IMA GRAMATIČKE POGREŠKE, pri čemu je **potrebno posebno** obratiti pažnju ako se pošiljatelj obraća u pogrešnom licu

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

Kako zaštiti e-mail adresu, Facebook račun i slično?

KORISTIMO RAZLIČITE LOZINKE ZA SERVISE NA INTERNETU (nemojmo koristiti istu lozinku za e-mail adresu, Facebook i druge stranice koje posjećujete). Kako ne bismo pamtili stotine lozinki, preporučuje se poslužiti programom za upravljanje lozinkama. Na ovoj poveznici možemo naći usporedbu takvih najpopularnijih aplikacija:

http://www.pcmag.com/article2/0,2817,2407168,00.asp

Ako se ista lozinka koristi na više mjesta, kriminalci to često koriste prokušanom metodom provale na slabo zaštićene stranice na kojima pokupe sve lozinke korisnika i potom ih isprobavaju na popularnijim internetskim stranicama ili servisima

KORISTIMO LOZINKE OD NAJMANJE OSAM ZNAKOVA KOJE SADRŽE VELIKA I MALA SLOVA, BROJEVE I SPECIJALNE ZNAKOVE. Nemojmo koristiti imena svojih bližnjih, ljubimaca i datume rođenja ljudi oko nas! Dodatni savjeti o lozinkama mogu se pronaći na:

http://csi.hr/p/najbolja%20lozinka

POPULARNE STRANICE I SERVISI POPUT FACEBOOKA, GOOGLEA I TWITTERA NUDE MOGUĆNOST TZV. POTVRDE U DVA KORAKA, koja štiti korisnički profil ili e-mail adresu od neovlaštenog upada jer šalje dodatni kod na naš mobitel koji treba unijeti ako se prijavljujemo s dotad nepoznatog uređaja.

Google / gmail – 2-Step verification https://www.google.com/landing/2step/
Twitter – Login Verification https://support.twitter.com/articles/20170388
Facebook – Login approvals http://www.oxhow.com/setup-facebook-login-approvals-two-step-verification-method/

BUDIMO OPREZNI KAD NAS PUTEM DRUŠTVENIH MREŽA KONTAKTIRAJU NEPOZNATE OSOBE. Prije nego što ih prihvatimo za prijatelje, provjerimo jesu li to zaista osobe za koje se predstavljaju. Primjerice uzmemo profilnu fotografiju i unesemo je u pretraživač Google jer prevaranti često koriste tuđe fotografije za lažne profile

Upute za pretraživanje koristeći fotografije: Kada smo na pretraživaču Google, 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 PODATKE POPUT E-MAIL ADRESE.

To je jedan od razloga zbog kojeg ćemo, prije ili poslije, biti meta onih koji žele zaraditi na nama **ili nas žele iskoristiti.** Neke od takvih osoba koriste internet i kao sredstvo upoznavanja s 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: „Nema takve stvari kao besplatan ručak". Drugim riječima, ako nešto zvuči predobro da bi bilo istinito – vjerojatno nije istinito!

Internetske prijevare također se mogu dogoditi putem aplikacija za komunikaciju poput Vibera, WhatsAppa ili drugih, gdje dobijemo poruku s poveznicom i tekstom koji nas informira **da smo nešto osvojili ili da samo trebamo posjetiti poveznicu** kako bismo 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 nas pokušati nagovoriti da otvorimo određenu stranicu ili skinemo neku datoteku.**

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! DODATAN OPREZ POTREBAN JE I KOD INSTALIRANJA RAZNIH APLIKACIJA, BILO NA PAMETNOM TELEFONU ILI FACEBOOKU. 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 BISMO JE TREBALI PREUZETI!

Internetski predatori

OVE OSOBE KORISTE INTERNET KAO SREDSTVO UPOZNAVANJA S DJECOM RADI USPOSTAVLJANJA KOMUNIKACIJE I USPOSTAVLJANJA ODNOSA. USPOSTAVLJENI ODNOS ZLOUPOTREBLJAVAJU S CILJEM SEKSUALNOG UZNEMIRAVANJA I ZLOSTAVLJANJA. NE POSTOJI TIPIČAN PREDATOR – RAZLIČITIH SU GODINA, SPOLA, STUPNJEVA OBRAZOVANJA I POSLA KOJIM SE BAVE. ALI NJIHOVO PONAŠANJE JE TIPIČNO:

- predstavlja se kao vršnjak ili poznanik
- predstavlja se kao prijatelj
- postavlja mnogo pitanja, a sam izbjegava ili daje lažne odgovore na pitanja njemu ili njoj
- želi se približiti sa zlom namjerom

KAKO SE MOŽEŠ ZAŠTITITI?

1. PRIPAZI ŠTO DIJELIŠ!
Ako su fotografije ili statusi koje podijeliš postavljeni na javno, može ih vidjeti svaki korisnik interneta.

2. PROVJERI SVAKOGA S KIM KOMUNICIRAŠ. Provjeri koristi li tuđe slike za svoj profil.

3. VJERUJ SVOM OSJEĆAJU.
Ako pomisliš da ti je nešto čudno ili ti se nešto ne sviđa, povjeri se svom roditelju ili odrasloj osobi od povjerenja i upitaj za savjet.

4. NIKAD NE PRIMAJ POKLONE!
Ako ti osoba koju si upoznao preko interneta želi kupovati igrice, skinove ili bilo koje druge poklone, moraš to reći roditeljima ili odrasloj osobi od povjerenja te razmisliti želi li ta osoba nešto zauzvrat!

5. NE NASJEDAJ NA LASKANJA!
lako je lijepo slušati dobre stvari o sebi, pripazi na pretjerano laskanje nepoznatih ljudi na internetu.

6. JEDNA OSOBA NE ZNA SVE!
Vrlo često internetski predatori žele te uvjeriti da su oni najpametniji, da te baš oni najviše razumiju i da su jedini koji su u pravu.

7. NEPOZNATIMA NE PRIČAJ O PRIVATNOM ŽIVOTU.
lako osoba možda izgleda kao netko koga znaš ili se pretvara da ti je prijatelj, nemoj dijeliti privatne stvari o sebi, svom životu, roditeljima ili obitelji.

8. INTIMNA PITANJA I FOTOGRAFIJE OSTAJU INTIMNA!
Intimne fotografije nemoj slati putem interneta ili mobilnih aplikacija. Svaka slika koju učitaš može završiti na internetu ili doći u ruke one osobe za koju to ne bi želio/željela.

9. NEKE FOTOGRAFIJE NIKAD NE DIJELI!
Fotografije sebe, intimne fotografije mlađe braće i sestara ili obitelji nisu nešto što bi bez dopuštenja roditelja trebalo objavljivati na internetu. Zapamti da takve slike svatko može preuzeti i proslijediti dalje.

10.NIKAD NEMOJ PRISTATI NA SASTANKE S NEPOZNATIM OSOBAMA bez znanja roditelja! Putem interneta i društvenih mreža upoznajemo puno novih osoba, no naći se u stvarnom životu s osobom koju smo upoznali preko interneta može biti poprilično opasno. Nikad na takve sastanke nemoj ići sam/a i uvijek razgovaraj sa svojim roditeljima prije nego što se odeš sresti s nepoznatom osobom.

5. ZAŠTITA OSOBNIH PODATAKA NA INTERNETU

PRIJE REGISTRACIJE NA DRUŠTVENOJ MREŽI TREBAMO PROČITATI POSTAVKE PRIVATNOSTI.

Problem se javlja u slučajevima kada se osobni podaci ostavljaju, međusobno razmjenjuju, prikupljaju ili šire dalje. **SVE NAVEDENO MOŽE UGROZITI PRIVATNOST PODATAKA.** Stoga, onda kada je primjereno, možemo se koristiti pseudonimom koji ne otkriva naše osobne podatke. Privatnost se može povezati uz anonimnost jer se anonimnost koristi kao instrument da se ostvari sloboda ili zaštiti privatnost osobe.

Roditelji, imajte na umu važnu činjenicu da i vaša djeca imaju pravo na privatnost!

Stoga ne objavljujte njihove fotografije na bilo kakvim mjestima. Primjerice na društvenim mrežama gdje se mogu iskoristiti ili zloupotrijebiti na način da iste posluže kao korisne informacije za pristup privatnim bazama podataka.

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

DRUŠTVENE MREŽE I PROGRAMI ZA RAZMJENU PORUKA

DANAŠNJA DJECA I MLADI TEŠKO MOGU ZAMISLITI ŽIVOT BEZ SVAKODNEVNOG KORIŠTENJA DRUŠTVENIH MREŽA POPUT FACEBOOKA, INSTAGRAMA ILI SNAPCHATA. PRAVILA LIJEPOG PONAŠANJA NA 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."

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.
- **Način komuniciranja potrebno je prilagoditi drugom korisniku ili grupi korisnika**
  kako bi razmjenjivanje informacija uspjelo.

- **Osigurajmo da se lokacija s fotografije ne može otkriti** korištenjem informacija s fotografije.

- **Ne otkrivajmo svoju lokaciju** ako nije potrebno, posebno privatne lokacije.

- **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 stvarate sliku o sebi nego utječete i na druge.

- **Ne sudjelujmo u nasilju putem interneta.** Ne omalovažavajmo i ne vrijeđajmo.

- **Roditeljima se ne preporučuje dijeliti fotografije svoje djece,** no ako ih dijelimo, ograničimo tko ih može vidjeti.

Poštujmo privatnost - kako vlastitu, tako i ostalih korisnika.

- **Ako koristimo javni ili tuđi uređaj** za pristup internetu, ne zaboravimo se odjaviti s aplikacija koje koristimo.

- **Nemojmo reagirati u ljutnji.**

- **Proučimo postavke za sigurnost i privatnost.** Maksimalno otežajmo neželjeno širenje naših privatnih informacija.

- **Poštujmo privatnost** - kako vlastitu, tako i ostalih korisnika.

- **Ponašanje na internetu ogledalo je korisnika.** Naše ponašanje utječe na ukupnu kvalitetu društvene mreže.

- **Ako je moguće, uključimo dvofaktornu autentifikaciju** - (dodatnu prijavu putem koda odaslanog na uređaj po izboru - najčešće naš mobilni uređaj)

FACEBOOK

FACEBOOK JE TRENUTAČNO NAJMASOVNIJA I NAJPOPULARNIJA DRUŠTVENA MREŽA S KOJOM JE VEĆINA KORISNIKA VEĆ UPOZNATA. IPAK, TREBA ZNATI DA INICIJALNO FACEBOOK ČINI LISTU NAŠIH PRIJATELJA JAVNO DOSTUPNOM (PUBLIC).

Kako bismo to promijenili, potrebno je otići pod **„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 zaštititi svoj Face možemo naći na poveznici

http://www.cert.hr/dokumenti/zastitite_privatnost_na_facebooku

INSTAGRAM

INSTAGRAM NAM OMOGUĆUJE DIJELITI I KOMENTIRATI FOTOGRAFIJE I VIDEOSADRŽAJ, OBRAĐIVATI FOTOGRAFIJE FILTRIMA 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 iskoristi netko zlonamjeran.

Kako zaštiti svoj Instagram profil?

1. 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).

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. PRIPAZIMO DA NISMO OTKRILI PREVIŠE PRIVATNIH INFORMACIJA u opisu svog profila, pogotovo ako to nije potrebno. Nema potrebe javno otkrivati osobne podatke kao što su naš datum rođenja, telefonski broj ili adresa.

4. PRIPAZIMO NA OTKRIVANJE LOKACIJE – na svakoj fotografiji koju stavimo na Instagram može se ukloniti lokacija tako da odaberemo fotografiju i u lijevom kutu pritiskom na lokaciju odaberemo prazno polje. Dodatno, na svom telefonu možemo zabraniti Instagramu da koristi čitanje lokacije.

5. UKLJUČIMO ODOBRAVANJE OZNAČAVANJA U TUĐIM FOTOGRAFIJAMA (TAGGING). Time ćemo moći odobriti koje se tuđe fotografije s nama mogu pojavljivati na našem profilu.

6. 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-Facor Authentication“.

SNAPCHAT

SNAPCHAT JE JOŠ JEDNA POPULARNA DRUŠTVENA MREŽA, NO I OVDJE TREBA BITI OPREZAN.

Razlika u odnosu na slične mreže jest da se poruke nakon čitanja brišu. Da budemo sigurniji i zaštitimo svoju i tuđu privatnost, poželjno je osigurati ga na idući način:

1. UKLJUČIMO „LOGIN VERIFICATION“ koja dodaje sigurnost našem Snapchatu tako da će Snapchat kad god se prijavljujemo s novog/nepoznatog uređaja SMS-om poslati kod na naš mobitel, koji potom trebati upisati prije nego što se Snapchat pokrene

• Pod opcijama (Settings) pronađimo **„Login Verification“** i odaberimo želimo li primati kodove SMS-om ili ih generirati aplikacijom na mobitelu

2. OSIGURAJMO SE DA NAS SAMO NAŠI PRIJATELJI MOGU KONTAKTIRATI PUTEM SNAPCHATA.

• pod opcijama (Settings) pronađimo „Contact Me“ i odaberimo **„My Friends“**

3. OGRANIČIMO TKO MOŽE VIDJETI NAŠU PRIČU (MY STORY)

• pod opcijama (Settings) pronađimo „View My Story“ i odaberimo **„My Friends“**

4. OGRANIČIMO TKO MOŽE VIDJETI GDJE SMO, TJ. NAŠU LOKACIJU

• pod opcijama (Settings) pronađimo „See My Location“ i odaberimo „My Friends“ ili još bolje **„Ghost Mode“** – (mogućnost neprikazivanja lokacije)

5. OBRATIMO PAŽNJU NA OBAVIJESTI ZA VRIJEME KOMUNIKACIJE PUTEM SNAPCHATA – Snapchat će nam javiti ako je netko s druge strane napravio screenshot naše poruke

6. PRIPAZIMO NA JAVNO DIJELJENJE SVOG SNAPCHAT KORISNIČKOG IMENA, čak i ako smo ograničili tko nas može kontaktirati

7. 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. NARAVNO, UVIJEK PRIPAZIMO ŠALJEMO LI PRAVOJ OSOBI PORUKU

YOUTUBE ZAŠTITA:

• **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

• Nakon što je video objavljen na mreži, nikada **NE ZNAMO TKO BI GA MOGAO VIDJETI.** Ako je kopiran ili ponovno objavljen, možda nećemo moći ukloniti svaku kopiju s interneta.

• **NEMOJMO ODAVATI PREVIŠE INFORMACIJE O SEBI I SVOJOJ OBITELJI** – druge se ne tiču naš broj mobitela ili druge osobne informacije; primjerice, pripazimo da se u našim videima nikad ne vidi prednja strana naše kuće

• **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**

KORISNE POVEZNICE

HAKOM
https://www.hakom.hr

Hrabri telefon
https://djeca.hrabritelefon.hr/ tel:116112

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

Centar za sigurniji internet
www.csi.hr

0800 606 606
besplatan i anoniman telefon za pomoć i podršku u slučaju nasilja na internetu.

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

EU Kids Online
www.hrkids.online

https://redbutton.mup.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

Što je to digitalni otisak?
https://www.csi.hr/p/%C5%A0to%20je%20to%20digitalni%20otisak%3F

Hakiran Facebook profil
https://www.csi.hr/p/Hakiran%20Facebook%20profil

Pet zlatnih pravila za roditelje na Internetu
https://www.csi.hr/p/5%20zlatnih%20pravila%20za%20pona%C5%A1anje%20na%20internetu

Najkorištenije aplikacije vaše djece
https://www.csi.hr/p/najkoristenije-aplikacije-koje-vase-dijete-koristi-162

Kako obrisati Facebook profil?
https://www.csi.hr/p/Kako%20obrisati%20Facebook%20profil%3F

Što je to spam?
https://www.csi.hr/p/%C5%A0to%20je%20to%20spam%3F

Zaštita djece na internetu
https://www.hakom.hr/default.aspx?id=337

[VIDEO] Zašto ne objavljivati slike djece na internetu
https://www.facebook.com/csihrv/videos/671407349676573/

Što je to cryptolocker virus i kako ga se riješiti?
https://www.csi.hr/p/%C5%A0to%20je%20to%20cryptolocker%20virus%20i%20kako%20ga%20se%20rije%C5%A1iti%3F

Što su to osobni podaci?
https://www.csi.hr/p/%C5%A0to%20su%20osobni%20podaci%3F

Video chat i web kamere
https://www.csi.hr/p/Video%20chat%20i%20web%20kamere

Kalkulator privatnosti
http://privatnost.hakom.hr/index.php

Katalog prevara na Internetu
http://privatnost.hakom.hr/catindex_hr.php

Minecraft vodič za roditelje
https://www.csi.hr/p/%C5%A0to%20je%20to%20Minecraft%3F%20Vodi%C4%8D%20za%20roditelje

Zaštitite svoju privatnost na Facebooku
http://cert.hr/dokumenti/zastitite_privatnost_na_facebooku