KAKO SE ZAŠTITITI

u svijetu interneta i mobilnih telefona

Kratki vodič za djecu i roditelje

(i sve koji žele znati više u digitalnom dobu)

HAKOM

Brzi razvoj tehnologije i pojava interneta povećali su broj faktora koji izravno utječu na razvoj i odrastanje djece i mladih. „Digitalno društvo“ ima nove načine pristupa informacijama, nove načine komuniciranja, provođenja slobodnog vremena, pa čak i nove načine kupovine, druženja, obrazovanja i obavljanja svakodnevnih zadataka u odnosu na nedavnu prošlost. 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 digitalnog doba.

ISTRAŽIVANJE EU KIDS ONLINE

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. Istraživanje je obuhvatilo 1017 djece u dobi od devet do 17 godina, kao i njihove roditelje. 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.

Svako sedmo dijete od devet do 17 godina u posljednjih se godinu dana susrelo s online prijateljem, odnosno osobom koju je upoznalo preko interneta. Većina djece susrela se s osobom svojih godina, dok se svako deseto dijete susrelo s osobom starijom od sebe. Gotovo polovina djece otišla je na sastanak uživo s jednim do dva online prijatelja, dok je 1/10 njih imala susrete s više od deset online prijatelja.

Svako četvrto dijete u dobi od devet do 14 godina i svako treće dijete u dobi od 15 do 17 godina je u potpunosti ili uglavnom zabrinuto 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.

U proteklih godinu dana više od pola djece u dobi od devet do 17 godina primilo je povrjeđujuću ili neprimjerenu poruku.

Svako 12. dijete u dobi od devet do 17 godina je u proteklih godinu dana primilo poruku sa seksualnim sadržajem. Poruke mogu uključivati riječi, slike ili video, a češće ih primaju starija djeca. Tri četvrtine djece koja su primila takve poruke dobila ih je putem društvenih mreža, gotovo polovina kao poruku poslanu na mobitel, a trećina putem pop-ups prozora i medijskih platformi.

Svako deseto dijete u dobi od 15 do 17 godina prihvaća sve zahtjeve za prijateljstvom drugih ljudi na društvenim mrežama.

IZVOR: HRKIDS.ONLINE

Nemojte ići sami na susrete s nepoznatim osobama koje ste upoznali online

1. ZAŠTITA OSOBNIH podataka na internetu

Prije registracije na društvenoj mreži važno je pročitati postavke privatnosti.

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 i ono prestaje biti intimno, privatno i tajno. Ovisno o tome kako nam je kreiran profil, ali i o samim osobitostima društvenih mreža te sadržaje mogu vidjeti, pa onda i komentirati i ljudi koje mi ne poznajemo i ne smatramo prijateljima. Onog trenutka kada nešto objavimo, bilo da se radi o nekoj anegdoti o nama ili našim fotografijama, mi više ne možemo kontrolirati koliko će „naših prijatelja" tu objavu podijeliti sa svojim internetskim prijateljima ili unutar grupa kojima pripadaju. Uljuljani u prividnu sigurnost društvene mreže, jer smo okruženi „prijateljima", često zaboravljamo da naši internetski prijatelji nisu uvijek ljudi koje dobro poznajemo ili neke od njih uopće ne poznajemo u stvarnom životu. Nažalost, postoje ljudi u internetskom prostoru koji nisu dobronamjerni i mogu grubo, ponižavajuće i nedobronamjerno komentirati ili zloupotrijebiti informacije.
OBJAVLJIVANJEM SLIKA SVOG DJETETA mi odlučujemo podijeliti svoje iskustvo i intimu s drugima. Međutim, tom odlukom i činom mi **OTKRIVAMO DJETETOVU INTIMU, UGROŽAVAMO DJETETOVU PRIVATNOST TE KREIRAMO NJEGOV „DIGITALNI OTISAK" BEZ NJEGOVA PRISTANKA.** Kako nad sadržajem jednom objavljenom na internetu više nemamo kontrolu, samim time ne znamo gdje se taj sadržaj može pojaviti. 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. Na neki način, učestalim objavljivanjem djetetovih fotografija i komentara kreiramo pred javnošću (prijateljima, obitelji, susjedima, odgajateljima, učiteljima...) sliku o djetetu, koja može biti drugačija od onog kakvo dijete jest i kako se ono samo želi predstavljati drugima u svom okruženju. Iskustva iz kliničke prakse pokazuju da posebno izlažuće za djecu može biti iznošenje podataka i komentara o osjetljivim obiteljskim krizama i teškim događajima na društvenim mrežama i u medijima, što roditelji znaju činiti iz svog osjećaja bespomoćnosti, frustracije i želje za podrškom. Ljudi, a posebno djeca, koji su doživjeli traumu ili prolaze obiteljsku i osobnu krizu su iznimno ranjivi i osjetljivi, tako da izloženost široj javnosti samo povećava mogućnost dodatne traumatizacije iznošenjem neprimjerenih informacija o privatnim i vrlo osobnim temama. Također, izlaganje djece u javnom prostoru, a društvene mreže to jesu, može izazvati jači osjećaj obilježenosti, ponekad jače negoli i sam događaj.
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 tako da iste posluže kao korisne informacije za pristup privatnim bazama podataka.

Nažalost, postoje ljudi u internetskom prostoru koji nisu dobronamjerni i mogu grubo, ponižavajuće i nedobronamjerno komentirati ili zloupotrijebiti informacije.

GDPR – Što je to?!

OD 25. SVIBNJA 2018. ZAŠTITA OSOBNIH PODATAKA I NA INTERNETU JE POSTALA 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.

GDPR se primjenjuje na sve koji obrađuju osobne podatke na teritoriju EU, ali i one koji izvan teritorija EU obrađuju osobne podatke građana EU.

GDPR uvodi određena nova prava, kao što je pravo da u svakom trenutku znamo tko i u koju svrhu obrađuje naše podatke, pravo na brisanje i ograničenje obrade podataka, te pravo na prigovor. GDPR propisuje da se smiju koristiti i obrađivati samo oni podaci koji su nužni i samo ako postoji određena svrha za obradu.

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, komu će biti dostavljeni te koja su njegova prava.

Zato je jako važno prije ostavljanja bilo kakvih osobnih podataka na internetu i društvenim mrežama dobro 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. INTERNETSKE TRGOVINE), PRIVOLU ZA OBRADU OSOBNIH PODATAKA DJETETA MLAĐEG OD 16 GODINA MOŽE DATI SAMO RODITELJ ILI SKRBNIK!

Djeci, mladima i roditeljima

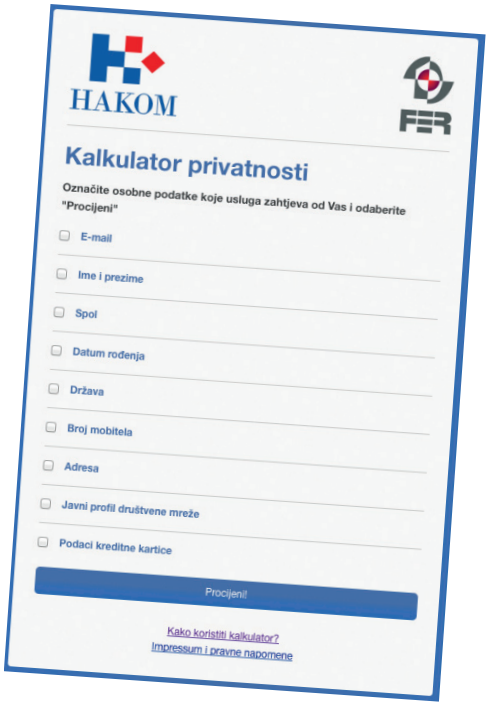
- **Nemojte javno objavljivati i razmjenjivati osobne i intimne podatke (lokaciju, fotografije, datum rođenja, adresu i slično)**
- **Ne objavljujte tuđe podatke (npr. fotografije prijatelja) bez suglasnosti te osobe**

Roditeljima

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

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/about.php

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**. Brojevi s kojih se šalju takve poruke će se nakon provjere u najkraćem roku blokirati.

Zabrana slanja i/ili primanja SMS i MMS poruka ili 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, jest 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, vršnjačko nasilje putem interneta sa sobom nosi nove opasnosti za žrtvu. 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 prividni osjećaj anonimnosti, mnogo snažniji 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 jer se naše društvo još ne zna nositi s ovakvim oblikom nasilja. 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 i dalje ne smatra da je nasilje putem interneta oblik nasilja koji može imati ozbiljne posljedice i 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.**

Jedna od najvažnijih karakteristika vršnjačkog nasilja putem interneta jest činjenica da ono nikad ne prestaje.

metode elektroničkog nasilja

Grubo online sukobljavanje

Kratkotrajna rasprava između dvije ili više osoba koju karakterizira ljut, eksplicitan i vulgaran govor, uvrede, a ponekad i prijetnje. Počinitelj nasilja ima za cilj izazvati bijes, tugu i/ili poniženje namjerno izazivajući sukob.

Uznemiravanje

Opetovano slanje okrutnih, uvredljivih, neprijateljskih i provokativnih poruka pojedincu/ki ili grupi. Najčešće se događa putem privatnih poruka, a cilj počinitelja nasilja je prijetnjom dovesti drugu osobu u ponižavajući i/ili podređeni položaj.

Ogovaranje i klevetanje

Izmišljanje informacija o žrtvi s ciljem povrede osobe i njihovo elektroničko slanje i dijeljenje. Uključuje stavljanje slike lica osobe na nepoznato golo tijelo i dijeljenje takve slike. Cilj ovih radnji je nanošenje štete žrtvinoj reputaciji ili uništavanje odnosa s drugim osobama.

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 što onda javno objavljuje ili dijeli dalje bez dopuštenja.

Socijalno isključivanje

Događa se jednako na internetu kao i u offline svijetu. Žrtve ne mogu ući u određene chat sobe ili ih se ne uključuje u grupne poruke.

Prijetnje i uhođenje

Opetovano slanje prijetećih poruka i neprestani pokušaji uspostavljanja i nastavljanja neželjenog kontakta zbog kojih se žrtva počinje bojati za osobnu sigurnost i dobrobit. Posebno je izraženo prilikom komunikacije s nepoznatim osobama i 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

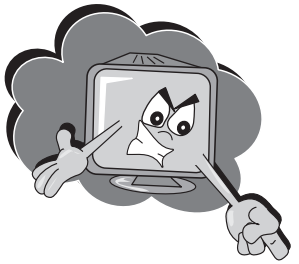
Znakovi koji ukazuju da je dijete možda doživjelo vršnjačko nasilje:

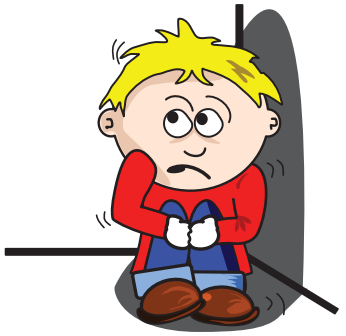
- učestala tišina
- povlačenje iz obiteljskih interakcija
- vidljiva tuga
- povlačenje od prijatelja i od aktivnosti u kojima je prije uživalo
- učestaliji izostanci iz škole (žaljenje na glavobolje i bolove u trbuhu)
- loš školski uspjeh (niže ocjene)
- gubitak apetita
- poremećaji spavanja (uključujući mokrenje u krevet)
- informacije iz škole o nenapisanim domaćim zadaćama ili problemima u ponašanju kao što su tučnjave s drugim učenicima
- prestaje koristiti računalo ili mobitel ili je povećano vrijeme provedeno na internetu u odnosu na prije
- čini se nervozno ili razdražljivo kada koristi računalo ili mobitel
- spominje nepoznate osobe
- pridaje sve veću važnost aktivnostima i osobama na internetu
- zatvara stranice, chatove i/ili skriva mobitel kad roditelji uđu u sobu ili se druga osoba približi
- stres prilikom čitanja poruka, odnosno primanja različitih sadržaja
- izbjegava razgovor 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 u 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





Znakovi koji ukazuju da se dijete možda nasilno ponaša:

- promjene u skupinama prijatelja (posebno gubitak skupine prijatelja)
- izražavanje nenaklonosti prema školi i učiteljima
- ima želju „praviti se važan“
- nabava predmeta ili dobara koje nije moglo kupiti bez roditeljskog znanja
- neobjašnjeni izljevi bijesa
- lako postaje frustrirano
- nerado radi domaću zadaću
- udara ili pokušava dominirati mlađom braćom i sestrama
- prestaje koristiti računalo ili mobitel (gasi ekran) kad se netko približi
- čini se nervozno ili razdražljivo kada koristi računalo ili mobitel
- skriva što radi na računalu ili mobitelu
- pretjerano provodi vrijeme uz mobitel ili računalo
- postaje nervozno ili ljutito kad mu se ograniči ili ukine korištenje računala ili mobitela

Znakovi koji ukazuju da se učenik/učenica možda nasilno ponaša:

- prkosan pogled nakon što ga/ju je učitelj opomenuo zbog ponašanja
- narušavanje rada u razredu
- otimanje, grabljenje ili uzimanje predmeta koji pripadaju drugim učenicima ili ih koriste drugi učenici
- udaranje i guranje drugih učenika
- ignoriranje učiteljeve upute da sluša ili da prestane pričati
- nevoljkost za aktivnim uključivanjem u razredne ili grupne aktivnosti
- ismijavanje drugih učenika kada govore
- nedostatak brige za školski i domaći rad

Kako roditelji mogu pomoći?

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.

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, prema njima se primjereno ponašati i od njih očekivati isto.

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 mnoštvo 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 pomoću kojih zaobilaze zaštitu naših računala.
U ovom trenutku, 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!**

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 svojih 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 s našim karticama, predstavljati se kao mi i slično.

Internetskim tražilicama poput Googlea ili Binga dostupno je manje od deset posto cijelog interneta

PRIMJER:

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

SAVJET:

u slučaju da primimo sličnu poruku, nije preporučljivo kliknuti na link, nego 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!

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

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!“**

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 SKYPEA**, no Skype ima domenu **@skype.com**, a ova poruka je došla s **@pmw.de**

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

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

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

Koristimo različite lozinke za servise na internetu (nemojte koristiti istu lozinku za e-mail adresu, Facebook i druge stranice koje posjećujete). Da ne biste 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 Googleov pretraživač jer prevaranti često koriste tuđe fotografije za lažne profile.

UPUTE ZA PRETRAŽIVANJE KORISTEĆI FOTOGRAFIJE:
kada smo na Googleovu 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 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. Takve osobe 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. 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!** 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 vas pokušati nagovoriti da otvorite određenu stranicu ili skinete neku datoteku.
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 biste ju trebali preuzeti!

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.

Ako dobijemo ponudu da ćemo nešto dobiti besplatno, trebamo razmisliti je li to vrijedno ostavljanja osobnih podataka.

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! Fotografije ili statuse koje podijeliš može vidjeti svaki korisnik interneta ako su postavljenje na javno.
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! Iako je lijepo slušati dobre stvari o sebi, pripazi na pretjerano laskanje nepoznatih ljudi na internetu.
6. Jedna osoba ne zna sve! Vrlo često te internetski predatori žele 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. Iako 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/la.
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.

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."

- **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 s 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. Tako ne samo što stvaramo sliku o sebi nego utječemo 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

- **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** ogledalo je 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)

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). Da biste to promijenili, potrebno je otići pod „Obitelj i odnosi“ (niže). 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

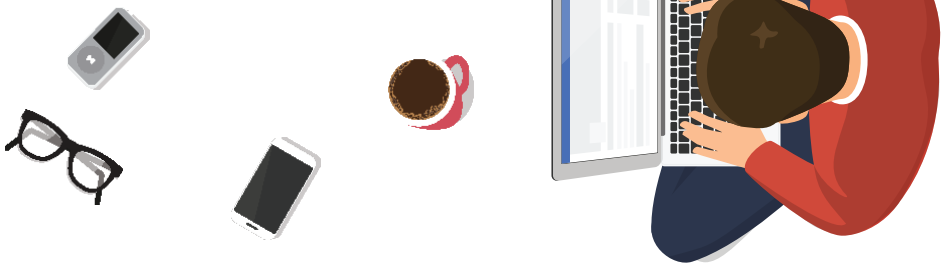
http://www.cert.hr/dokumenti/zastitite_privatnost_na_facebooku

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 netko zlonamjeran iskoristi.

Kako zaštiti svoj Instagram profil?

1. Da zaštitimo privatnost, možemo blokirati sljedbenike koje ne poznajemo: na listi sljedbenika odaberemo onoga 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, telefon 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)**. Tako 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-Factor 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 se na idući način:

1 Uključimo **„Login verification“** koja dodaje sigurnost našem Snapchatu tako da kad god se prijavljujemo na Snapchat s novog/nepoznatog uređaja, Snapchat će 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 ne prikazivanja 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 Pripazite na javno dijeljenje svog Snapchat korisničkog imena, čak i ako ste ograničili tko vas 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 nekomu i pokazujemo prijašnje poruke, one koje smo označili s **„My Eyes Only“** neće biti među njima
8 Naravno, uvijek pripazite šaljete 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 – drugih se ne tiče 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.

ponašanje

• Čak i ako nas nešto ljuti, **NEMOJMO REAGIRATI** na svaku poruku koju dobijemo – nasilnicima će prije dosaditi napadati nas ako se ne upuštamo u raspravu s njima
• **ZABRANIMO PRISTUP** osobama koje nas vrijeđaju ili povrijede
• **SPRIJEČIMO** opasne ili neugodne situacije: ne objavljujmo nešto samo zato što nas je netko drugi zamolio. Također, nemojte pokušavati susresti nikoga s kim ste se susreli/upoznali na internetu bez savjetovanja s pouzdanom odraslom osobom
• **IZRAVNO PRIJAVIMO** YouTubeu svaku osobu koja zlostavlja ili sadržaj koji stvara neugodu. YouTube će ih blokirati ako se ne ponašaju sukladno pravilima ponašanja. Imajmo na umu da su neka ponašanja na internetu i zakonom kažnjiva.
• **VODIMO RAČUNA O PRAVU DRUGIH** – ako 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 bismo željeli da vidi naša baka, učiteljica ili roditelj? Ako ne, onda vjerojatno nije dobra ideja objaviti takav video.

HAKOM https://**www.hakom.hr ,** e-mail: **zaštita-djece@hakom.hr**

Centar za sigurniji internet **www.csi.hr**

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

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

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

EU Kids Online **www.hrkids.online**

Ova brošura prvenstveno je namijenjena djeci u osnovnoj školi i njihovim roditeljima, ali može biti koristan izvor informacija svakomu tko želi više znati o temi ponašanja, sigurnosti i djece na internetu. Brošura je rezultat suradnje HAKOM-a, Centra za sigurniji internet i Ministarstva znanosti i obrazovanja.

HAKOM

csi.hr Centar za sigurniji internet

Ministarstvo znanosti i obrazovanja