#DeleteCyberbullying

Priručnik za učitelje

Sadržaj

Uvod : prezentacija aplikacije #DeleteCyberbullying app

#DeleteCyberbullying app interaktivni je kviz za tinejdžere, roditelje i učitelje koji prikazuje sadržaje ovisno o unesenim odgovorima na pitanja. Cilj je preusmjeriti korisnika na najrelevantnije izvore informacija, materijale ili čak na pristup telefonu za pomoć ako je korisnik žrtva cyberbullyinga.

Odgovori aplikacije automatski se prilagođavaju jeziku i državi korisnika, kroz partnerstvo s lokalnim organizacijama koje rade na problemu cyberbullyinga.

Dostupna je na Android platformi od lipnja 2014. i za iOS (iPhone, iPad) od rujna 2014. Aplikacija je prvo objavljenja u sljedećim zemljama (na službenom jeziku države): Belgija, Francuska, Velika Britanija, Irska, Nizozemska, Finska, Danska, Grčka, Bugarska, Španjolska, Hrvatska, Njemačka, Švedska i Mađarska.

Ostali dijelovi aplikacije su sljedeći:

- Integrirani video namijenjen podizanju svijesti o cyberbullyingu.
- "Gumb za pomoć" u slučaju da korisnik treba izravnu pomoć.
- Informacije o projektu u dijelu "Novosti" s najnovijim vijestima o projektu Delete Cyberbullying.

Svrha našeg projekta je osigurati masovno preuzimanje aplikacije i uporabu od strane tinejdžera (u dobi od 12 do 18), roditelja i učitelja, kako bismo povećali njihovu osviještenost o problemu, doprinijeli sprječavanju cyberbullyinga i postali jedinstveni portal za pristup informacijama o cyberbullyingu u državi korisnika i na jeziku na kojem mu može biti pružena izravna pomoć ako je potrebno.

Aplikacija je dostupna na sljedećim jezicima: engleski, francuski, njemački, španjolski, finski, mađarski, bugarski, nizozemski, hrvatski, grčki, švedski i danski.

Prijedlog za korištenje u okviru nastavne jedinice ili aktivnosti o cyberbullyingu

Preporučljivo je ohrabriti učenike da preuzmu aplikaciju i koriste je nekoliko dana prije aktivnosti ili nastavne jedinice. Učenici trebaju odgovoriti na pitanja iz kviza "A ti?" najmanje jednom, i najmanje tri puta na pitanja iz kviza "Provjeri svoje znanje" kako bi prošli dovoljan broj različitih odgovora.

Učenici također, trebaju napisati tri primjedbe, opažanja ili pitanja o temama o kojima bi htjeli razgovarati vezano uz kvizove na aplikaciji. Za vrijeme nastave, učenici će imati priliku podijeliti svoja razmišljanja s ostalima u razredu.

Kako koristiti ovaj priručnik

Ovaj priručnik sadrži niz aktivnosti ili nastavnih jedinica o pojedinim temama vezanima uz cyberbullying. One su ili izravno vezane uz cyberbullying (definicija, kako reagirati...) ili neizravno (zaštita privatnosti, digitalne vještine...). Kako biste nastavu mogli prilagoditi interesima, primjedbama i pitanjima učenika, aktivnosti i nastavne jedinice su modularne i mogu se koristiti pojedinačno i bilo kojim redoslijedom. Preporučuje se, međutim, započeti prvom aktivnošću o definiciji cyberbullyinga.

Aktivnosti/nastavne jedinice su samo općenite smjernice i ne mogu predstavljati sveobuhvatni nastavni plan o cyberbullyingu. Aplikacija i popis pitanja mogu poslužiti i samo kao "inicijator lekcije" iz kojeg će učitelj razviti svoj vlastiti plan poučavanja.

Svaka aktivnost/nastavna jedinica će uključivati:

- upućivanje na pitanja u aplikaciji koja su vezana uz temu (vidi popis pitanja u dodatku),
- upute vezane uz trajanje i ciljane dobne skupine,
- ostale aktivnosti/nastavne jedinice koje treba raspraviti s učenicima prethodno (pripremne aktivnosti),
- ostale aktivnosti/nastavne jedinice koje su vezane i mogu biti razvijene paralelno ili u kasnijoj fazi,
- kratki sažetak koji govori o značaju aktivnosti/nastavne jedinice i očekivanim ishodima učenja.

Razredne aktivnosti i pripreme za nastavu

Aktivnost 1: *Što je cyberbullying?*

Pitanje iz aplikacije: pitanje 1 iz kviza "Provjeri svoje znanje".

Trajanje: 15 minuta.

Dobna skupina: 10-18.

Domaći uradak: nema.

Priprema: nema.

Slične aktivnosti: aktivnosti 2 i 3.

Ciljevi: razviti opće razumijevanje o cyberbullyingu, njegovim karakteristikama i osposobiti se za prepoznavanje ako/kada ga učenici vide/iskuse.

Papirnata verzija:

Zamolite učenike da uzmu komad papira i zapišu što misle koja četiri obilježja definiraju cyberbullying. (2 minute)

Neka učenici dobrovoljci ili oni koje ste izabrali pročitaju naglas što su napisali, a glavne ideje grupirajte i zapišite na ploču. (6 minuta)

Zatim, pitajte učenike nedostaje li nešto obilježjima koje ste zapisali na ploči. (2 minute)

Iskoristite preostalo vrijeme kako biste nadopunili ili komentirali obilježja koja su učenici predložili. (5 minuta)

On line digitalna verzija:

Kreirajte Google Docs obrazac s pitanjem "Napišite nekoliko ključnih riječi koje po vama opisuju glavna obilježja cyberbullyinga." (prije nastavnog sata)

Podijelite poveznicu sa svim učenicima i zamolite ih da popune obrazac svojim odgovorima. Izvezite Google doc sadržaj i zalijepite ga u word cloud uslugu poput "Wordle". http://www.wordle.net/create (3 minute)

Projicirajte word cloud na bijelu ploču i zamolite učenike da rasprave ono što je prikazano, na primjer, koje se riječi najviše ponavljaju i nedostaje li nešto na popisu. (7 minuta)

Iskoristite preostalo vrijeme kako biste nadopunili ili komentirali obilježja koja su učenici predložili uz pomoć opisa karakteristika prikazanih u nastavku. (5 minuta)

Cyberbullying ima mnogo "službenih" definicija. Iako se definicije razlikuju, postoji niz deskriptora za bullying i cyberbullying:

- Prvo, ideja da počinitelj **ima namjeru povrijediti žrtvu,** bilo emocionalno ili fizički.
- Drugo, da postoji **neravnoteža moći** između počinitelja i žrtve. To je kod klasičnog bullyinga lako uočiti, ali je teže definirati u svijetu interneta. Dokaz te neravnoteže

moći može ležati u činjenici da nasilnik ili nasilnici često ostaju anonimni i imaju veliku moć kad gotovo u trenu imaju pristup široj publici dok objavljuju materijal koji može nekoga osramotiti ili povrijediti.

- Treće, uvijek postoji element **ponavljanja ili kontinuirane prijetnje daljnjom agresijom.** Cyberbullying i/ili bullying nisu jednokratni komentari ili prijetnje, koje nazivamo "flaming" 1, "trolling" 2 ili jednostavno jednokratna agresija 3. Treba, međutim, biti oprezan jer u svijetu interneta, jednokratna agresija koja dolazi od strane više korisnika ili istog korisnika, ali se masovno dijeli s drugima u stvari postaje cyberbullying.
- Napokon, najočitije obilježje cyberbullyinga jest da uključuje uporabu **informacijske i komunikacijske tehnologije** (poput pametnih telefona, računala, tableta...) i naročito **internet.**

Vrijedno je spomena kako je **vrlo teško razlikovati cyberbullying od spolnog uznemiravanja, cyber uhođivanja i ostalih sličnih ponašanja.** Cyberbullying može imati oblik spolnog uznemiravanja, na primjer komentiranje tijela, izgleda ili spola/roda, prosljeđivanje intimnih slika (seksualni sadržaj, golo tijelo/dijelovi tijela) ili video snimaka, širenje glasina itd. Sve te radnje mogu se smatrati cyberbullyingom i spolnim uznemiravanjem.

No, uočavanje razlika manje je važno, najvažnije je prepoznati da **krajnji učinak** može biti isti (vidi aktivnost 2 o posljedicama cyberbullyinga) te će koraci koje žrtva treba poduzeti uglavnom trebati biti jednaki (vidi aktivnost 3 o tome kako reagirati na cyberbullying).

Aktivnost 2: Što je tako posebno kod cyberbullyinga?

Pitanje iz aplikacije: pitanja 1,6,14,15 i 23 iz kviza "Provjeri svoje znanje" i pitanja 2-9 i 11 iz "A ti?" kviza.

Trajanje: 20 minuta.

Dobna skupina: 10-18.

Domaći uradak: nema.

Priprema: aktivnost 1.

Slične aktivnosti: aktivnosti 3,4 i 6.

Ciljevi: utvrditi razlike između bullyinga i cyberbullyinga, razumjeti zbog čega je cyberbullying tako ozbiljna stvar.

[1] http://en.wikipedia.org/wiki/Flaming_%28Internet%29

[2] Mnogi termini kao "trolling" ili "flaming" su u nastajanju i mogu imati različita značenja ovisno o kulturi. Trolling je u nekim slučajevima sličan cyberbullyingu. Flaming se obično smatra ispadom mržnje ili agresije na chatu, forumu ili društvenim mrežama, često zbog kontroverznih tema. Trolling se obično razumijeva kao stvaranje nesklada započinjanjem sukoba ili uznemiravanjem ljudi.

[3] Des Butler, Sally Kift & Marilyn Campbell , "Cyber Bullying In Schools and the Law: Is There an Effective Means of Addressing the Power Imbalance?", *eLaw Journal: Murdoch University Electronic Journal of Law*, Vol 16, No 1 (2009), p. 85-86.

Online domaća zadaća i lekcija:

Pripremite kratku online anketu za svoje učenike, koristeći Google obrasce ili neki drugi alat za kreiranje online anketa, sa sljedećih 5 pitanja (slažem se/ne slažem se):

- Bullying je gori od cyberbullyinga zbog toga što može doći do fizičkih ozljeda.
- Cyberbullying je gori od bullyinga zbog toga što se širi puno brže među puno širom publikom.
- Bullying je gori nego cyberbullying zbog toga što može dovesti do krađe važnih predmeta kao što su novčanik, telefon, sat...
- Cyberbulling je gori od bullyinga zbog toga što može trajati 24 sata dnevno, čak i kod kuće gdje biste se trebali osjećati sigurnima.
- Cyberbullying i bullying nemaju nikakve veze jedno s drugim.

Za svako od ovih pitanja, neka učenici zapišu razloge zbog kojih se slažu/ne slažu sa svakom od ovih tvrdnji.

Na satu, projicirajte rezultate kviza i raspravite svako pitanje s učenicima. (15 minuta)

Na kraju sata, navedite ključne razlike između bullyinga i cyberbullyinga koje su navedene u nastavku. (5 minuta)

Offline lekcija:

Zamolite učenike da rade u grupi od troje ili četvero i izaberu jednu od navedenih dviju tvrdnji za koju će navesti tri argumenta koja ih brane: bullying je gori od cyberbullyinga ili cyberbullying je gori od bullyinga. (3 minuta)

Zamolite dobrovoljce da se jave ili izaberite dvije grupe koje brane oprečne ideje (ako je moguće) i neka predstave svoje argumente kroz debatu. Na kraju debate, zamolite ostale učenike da glasuju tko je imao najuvjerljivije argumente. U slučaju da sve grupe odluče braniti istu ideju, neka se dvije grupe predstave i neka učenici glasuju za grupu koja je imala najuvjerljiviju i najpotpuniju prezentaciju. (10 minuta)

Sažmite ideje iz debate i predstavite neke ključne razlike između bullyinga i cyberbullyinga. (5 minuta)

Zbog čega je cyberbullying tako poseban? Zašto je to tako ozbiljna stvar? Što se može smatrati gorim od bullyinga?

Može li cyberbullying biti štetniji od bullyinga u fizičkom svijetu?

- Cyberbullying može trajati **24 sata dnevno, svaki dan i na svakom mjestu** (u domu žrtve na primjer, ugrožava svaki osjećaj sigurnosti pa čak i u vlastitom domu)
- **Potencijalna publika** među kojom kruže ponižavajuće i štetne slike, tekstovi, video materijali **je ogromna** i **širenje je gotovo trenutačno.**
- **Brisanje štetnog materijala može biti teško** iako ne i nemoguće. Pružatelji usluga na internetu poput društvenih mreža ili blogova su relativno neučinkoviti u trajnom uklanjanju materijala cyberbullyinga na vrijeme (kao što se to radi s krivotvorenim materijalom), a originalna kopija materijala može se postaviti na druge platforme ili ponovno objaviti i nakon brisanja.

- Cyberbully ima osjećaj da **može ostati anoniman**, a iako je to moguće, **jasno i precizno identificirati počinitelja(e)** je **jako teško**. Ponekad, cyberbully niti ne poznaje žrtvu i obratno!
- Cyberbullying može biti i okrutniji zbog toga što **bully ne može vidjeti trenutnu reakciju žrtve i osjetiti empatiju, krivnju ili se uvjeriti da je pretjerao/la.** Žrtva može jako patiti zbog toga što ne zna koliko ljudi je uključeno, jesu li njihovi prijatelji iz razreda vidjeli štetnu poruku, sliku i video i kako su reagirali. To često rezultira izbjegavanjem pohađanja škole.
- Zbog toga što je različit od klasičnog bullyinga, mnogo **mjera protiv cyberbullyinga koje poduzimaju odrasli mogu još pogoršati stvari.** Na primjer, zabrana pristupa internetu (oduzimanje kompjutora, pametnog telefona...) ili brisanje štetnih poruka ili materijala samo pogoršava stvari. Cyberbullying ne prestaje zbog toga što žrtve nemaju pristup internetu ili zbog toga što je nešto materijala izbrisano, to samo pogoršava osjećaj bespomoćnosti žrtve koja je prepuštena zamišljanju strahota koje se dijele online, a osim toga, to otežava istragu cyberbullyinga i identifikaciju počinitelja.
- Za razliku od bullyinga, **"znakove" cyberbullyinga teže je prepoznati**, što okolini otežava prepoznavanje žrtve i pružanje pomoći. Dok bullying često iza sebe ostavlja fizičke tragove i dokaze koje je relativno lako uočiti (slomljena i ukradena roba, tragovi fizičke agresije...), cyberbullying se može uočiti jedino oduzimanjem elektroničkih uređaja u vlasništvu žrtve te proučavanjem njegovih/njenih računa, poruka, itd., čime se krše prava na zaštitu privatnosti.

Napomena: Razlike između cyberbullyinga i bullyinga koje smo opisali nemaju svrhu umanjiti značaj i ozbiljnost bullyinga. One su namijenjene isticanju nekih ključnih razlika između to dvoje. U konačnici, svaki će pojedinac biti povrijeđen na svoj način bilo kroz bullying ili cyberbullying.

Aktivnost 3: Posljedice cyberbullyinga

Pitanje iz aplikacije: pitanje 3,6,7 i 10 iz kviza "Provjeri svoje znanje".

Trajanje: 25 minuta.

Dobna skupina: 10-18.

Domaći uradak: nema.

Priprema: aktivnost 1.

Slične aktivnosti: aktivnosti 2 i 4.

Ciljevi: naučiti nešto o ozbiljnosti cyberbullyinga i pravnim posljedicama.

Zamolite učenike da se podijele u parove. Jedan učenik će igrati ulogu počinitelja cyberbullyinga, a drugi ulogu žrtve. Zatražite da smisle najmanje 5 situacija cyberbullyinga u kojima počinitelj čita opisanu situaciju cyberbullyinga, posljedice, moguće pravne implikacije, reakcije žrtve te kako bi to utjecalo na nju. U slučaju da učenicima treba dodatna inspiracija možete im pomoći tako što ćete napraviti popis mogućih situacija uz pomoć Dodatka 1 (popis pitanja iz odjeljka "jeste li iskusili") (5 minuta)

Pozovite dobrovoljce ili odaberite jedan par učenika da odigraju različite situacije u stilu "forum teatra"[4]. Nakon svake odigrane situacije zamolite publiku (ostatak učenika) da komentira dva aspekta: što bi mogle biti posljedice ovih postupaka za počinitelja i kako bi mogle utjecati na žrtvu. (12 minuta)

Podijelite članke iz novina iz Dodatka 2 i neka ih učenici pročitaju (3 minute).

Ostatak vremena iskoristite za raspravu o sadržaju članka i upotpunite njihova razmišljanja o posljedicama cyberbullyinga za žrtvu i počinitelje elementima prikazanima u nastavku. (5 minuta)

Istraživanja ukazuju na mnogo ozbiljnih posljedica za **žrtvu:**

- **negativne emocionalne reakcije** poput straha, ljutnje, tuge, frustracije, bespomoćnosti, nižeg samopoštovanja i samopouzdanja, depresije;
- **negativna ponašanja** poput izoliranja, nedostatka koncentracije, lošijih rezultata u školi, izostajanja iz škole, delinkvencije, osvete i odmazde protiv cyberbullyija ili nekog drugog,
- **ekstremne reakcije** poput samoozljeđivanja, pokušaja samoubojstva ili izvršenja samoubojstva.

Te posljedice povezane su s prirodom cyberbullyinga koja je prikazana u aktivnosti 2 (cyberbullying može trajati 24 sata dnevno, žrtva se osjeća bespomoćno... vidi gore).

Osim zakona na nacionalnoj razini koji reguliraju **uznemiravanje**, **Direktiva o zaštiti privatnih podataka (95/46/EC)** koja se primjenjuje u svim zemljama članicama EZ, također, može poslužiti kao pravna osnova za borbu protiv cyberbullyinga. Zaštita osobnih podataka igra važnu ulogu jer "kadgod se osobni podaci pojedinaca prikupljaju elektronički; npr. na internetskim forumima, društvenim mrežama, putem instant poruka ili komunikacije e-poštom, zakonodavstvo nalaže da oni koji (...) objavljuju podatke o trećim osobama moraju poštovati razna načela."[5]

To znači da kadgod cyberbully razotkriva osobne podatke žrtve, odredbe Direktive EZ o zaštiti osobnih podataka primjenjuju se u potpunosti, s obzirom na to da je objava takvih informacija zahtijeva prethodni pristanak osobe. Odgovornost, dakle, leži u rukama cyberbullyia koji, obradom i objavljivanjem osobnih podataka, postaje "upravitelj podataka" i kao takav, snosi ozbiljne pravne posljedice. Presuda Europskog suda pravde iz 2003. g. u slučaju Lindqvist [6] potvrdila je ovakvo tumačenje.

Žrtve mogu, temeljem tog zakona, podnijeti prigovor zbog kršenja njihovih prava na zaštitu osobnih podataka, bilo sudu ili drugom nadležnom tijelu koje nadzire zaštitu podataka.

[4] http://en.wikipedia.org/wiki/Forum_theatre

[5] Giovanni Buttarelli, "Data protection legislation in Europe, preventing cyber-harassment by protecting personal data and privacy", 07/06/2010, http://www.edps.europa.eu/EDPSWEB/webdav/shared/Documents/EDPS/Publications/Speeches/2010/10-06-07_Speech_Cyber-harassment_EN.pdf

[6] http://curia.europa.eu/juris/liste.jsf?language=en&num=C-101/01

Aktivnost 4: Što raditi u slučaju pojave cyberbullyinga?

Pitanje iz aplikacije: pitanje 4 i 5 iz kviza "Provjeri svoje znanje".

Trajanje: 30 minuta

Dobna skupina: 10-18

Domaći uradak: nema.

Priprema: aktivnost 1.

Slične aktivnosti: aktivnosti 2 i 3.

Ciljevi: steći osnovno znanje o tome kako reagirati u slučaju cyberbullyinga ako ste žrtva ili promatrač (svjedok).

Zamolite učenike da rade u grupama od tri ili četiri člana i dajte im uputu da izrade petominutni skeč o tome kako bi reagirali u tri različite situacije cyberbullyinga, jedan učenik treba biti žrtva, a ostali promatrači (svjedoci). U slučaju da učenicima treba dodatna inspiracija možete im pomoći tako što ćete napraviti popis mogućih situacija uz pomoć Dodatka 1 (popis pitanja iz odjeljka "jeste li iskusili") (5 minuta)

Zamolite dobrovoljce ili izaberite dvije grupe koje će predstaviti moguće reakcije na tri situacije cyberbullyinga na koje su naišli. Nakon skeča ostavite nešto vremena za komentare cijelog razreda (15 minuta)

Na temelju dvije prezentacije, zamolite učenike da odrede ključne savjete za promatrače i žrtve cyberbullyinga. (5 minuta)

Prikažite učenicima #DeleteCyberbullying video na You Tubeu (3 minuta)

https://www.youtube.com/watch?v=dkG00Czb4ho&list=UUSfCFQvV7annlf60sjxGGTQ

Nadopunite savjete učenika nekim od sljedećih savjeta kako se odnositi prema cyberbullyingu iz pozicije žrtve i promatrača. (2 minute)

Najčešći savjeti žrtvama cyberbullyinga su:

- **Ne reagiraj** na cyberbullying poruke i **ne prosljeđuj ih**, a pogotovo nemoj **uzvraćati cyberbullyingom** (to obično pogoršava stvari);
- **Sačuvaj dokaze** cyberbullyinga (print screen, spremi na tvrdi disk, zabilježi datume i vrijeme cyberbullyinga,… sve to je potrebno za dokazivanje cyberbullyinga u slučaju službene istrage);
- **Blokiraj bullyija i daj mu/njoj do znanja da znaš da je on/ona ta/j koji vas povređuje i zatražite da prestane** (iako to možda neće imati nikakav učinak na cyberbullyija ili više njih, to je također dio standardne procedure koji se mora učiniti kako bi se problem stavio pred upravu škole ili čak policiju);
- **Prijavite incident administratoru internetske stranice** (društvene mreže, platforme za dijeljenje videa trebale bi imati način za prijavu cyberbullyinga: čak iako nisu uvijek 100% učinkoviti, to je standardna procedura koju treba odraditi);

- **Razgovaraj s odraslom osobom kojoj vjeruješ** (s roditeljima, učiteljicom ili bilo kojom drugom odraslom osobom) **ili s prijateljem/icom od povjerenja;**
- **Nazovi telefon za pomoć** u svojoj zemlji ako želiš razgovarati o nekom specifičnom problemu (vidi #DeleteCyberbullying app za stupanje u kontakt s telefonom za pomoć);
- **Obavijesti policiju** uz pomoć odrasle osobe kojoj vjeruješ ako cyberbullying ne prestane.

Promatrači mogu biti vršnjaci, ali isto tako i neke druge osobe koje su svjedočile cyberbullyingu (trenutku slanja ili objavljivanja ili zaprimanja poruke od strane žrtve).

Iako su promatrači obično pasivni i nisu voljni uključiti se zbog straha da se cyberbulling (ili bullying) ne okrene prema njima, njihova uloga je ključna za rano otkrivanje i intervenciju cyberbullyinga. Ono što oni mogu slično je onom što smo već opisali:

- zabilježite/sačuvajte ono čemu ste svjedočili kao dokaz cyberbullyinga;
- založite se za žrtvu i jasno izrazite svoje neslaganje s ponašanjem cyberbullyija;
- razgovarajte o tome čemu ste svjedočili s odraslom osobom kojoj vjerujete;
- nikad ne ohrabrujte ili ne doprinosite indirektno cyberbullyingu (prosljeđivanje poruke; "lajkanje" neprimjerenih uvredljivih šala...)

Aktivnost 5: Privatnost na internetu, čemu uzrujavanje?

Pitanje iz aplikacije: pitanja 9,11,17-21 i 23 iz kviza "Provjeri svoje znanje" i pitanja 3,4 i 7 iz "A ti?" kviza.

Trajanje: 35 minuta.

Dobna skupina: 14-18.

Domaća zadaća: prije sata, zatražite učenike da istraže vijesti vezane uz pitanja zaštite privatnosti na internetu.

Priprema: nema.

Slične aktivnosti: aktivnosti 6 i 7.

Ciljevi: razumjeti implikacije pretjeranog dijeljenja informacija na internetu i zbog čega je važno razmisliti prije nego što nešto objavite.

Prije nastavnog sata, zamolite učenike da istraže priče u novinama o kršenju privatnosti na internetu u posljednjih nekoliko mjeseci i da odgovore na sljedeća pitanja:

- Jeste li već prije čuli za takvu priču?
- Što biste vi učinili u sličnoj situaciji?
- Što mislite na koji se način promijenio pojam privatnosti razvojem tehnologije i interneta?
- Mislite li da bismo trebali mijenjati naša ponašanja ili društvena pravila?

Za vrijeme sata, zamolite dobrovoljce ili izaberite učenike koji će prezentirati svoje misli i pokrenite raspravu o posljednja dva pitanja. Ohrabrite ostale učenike iz razreda da se uključe u raspravu. Za četvrto pitanje, naročito, možete organizirati parlamentarnu raspravu. Podijelite razred na dva dijela, s jedne strane neka budu učenici koji žele zastupati mišljenje kako bismo uglavnom trebali mijenjati svoje ponašanje na internetu i način na koji koristimo nove tehnologije (društvene norme ostaju iste, ali mi trebamo naučiti mudrije koristiti tehnologije i internet), a s druge strane neka budu učenici koji žele braniti mišljenje kako se naše društvena pravila trebaju mijenjati i prilagoditi novim tehnologijama i internetu (neki pojmovi poput privatnosti ne mogu ostati isti). Pokušajte da obje skupine imaju otprilike jednak broj učenika, a vi preuzmite ulogu moderatora. (20 minuta)

Ako želite, možete podijeliti članke iz Dodatka 3 i ukratko ih analizirati s učenicima, pokazujući kako kršenje privatnosti na internetu može imati vrlo širok raspon posljedica od gubitka zaposlenja do pljačke, itd. (5 minuta).

Na kraju rasprave, možete podijeliti Dodatak 4, to je dokument koji je pripremio Europski parlament i sadrži 10 savjeta o tome kako se zaštititi na internetu. Neka ih učenici pročitaju i ukratko iznesu svoja razmišljanja o njima. (10 minuta)

Aktivnost 6: Kako funkcionira internet?

Pitanje iz aplikacije: pitanje 13,14,15,22 i 28 iz kviza "Provjeri svoje znanje".

Trajanje: 40 minuta.

Dobna skupina: 12-18.

Domaća zadaća: nakon sata, zamolite učenike da pronađu nešto o "hops" (preskocima) i pristupanju materijalu na internetu.

Priprema: nema.

Slične aktivnosti: aktivnosti 5 i 7.

Ciljevi: razumjeti osnove funkcioniranja interneta i neke od implikacija.

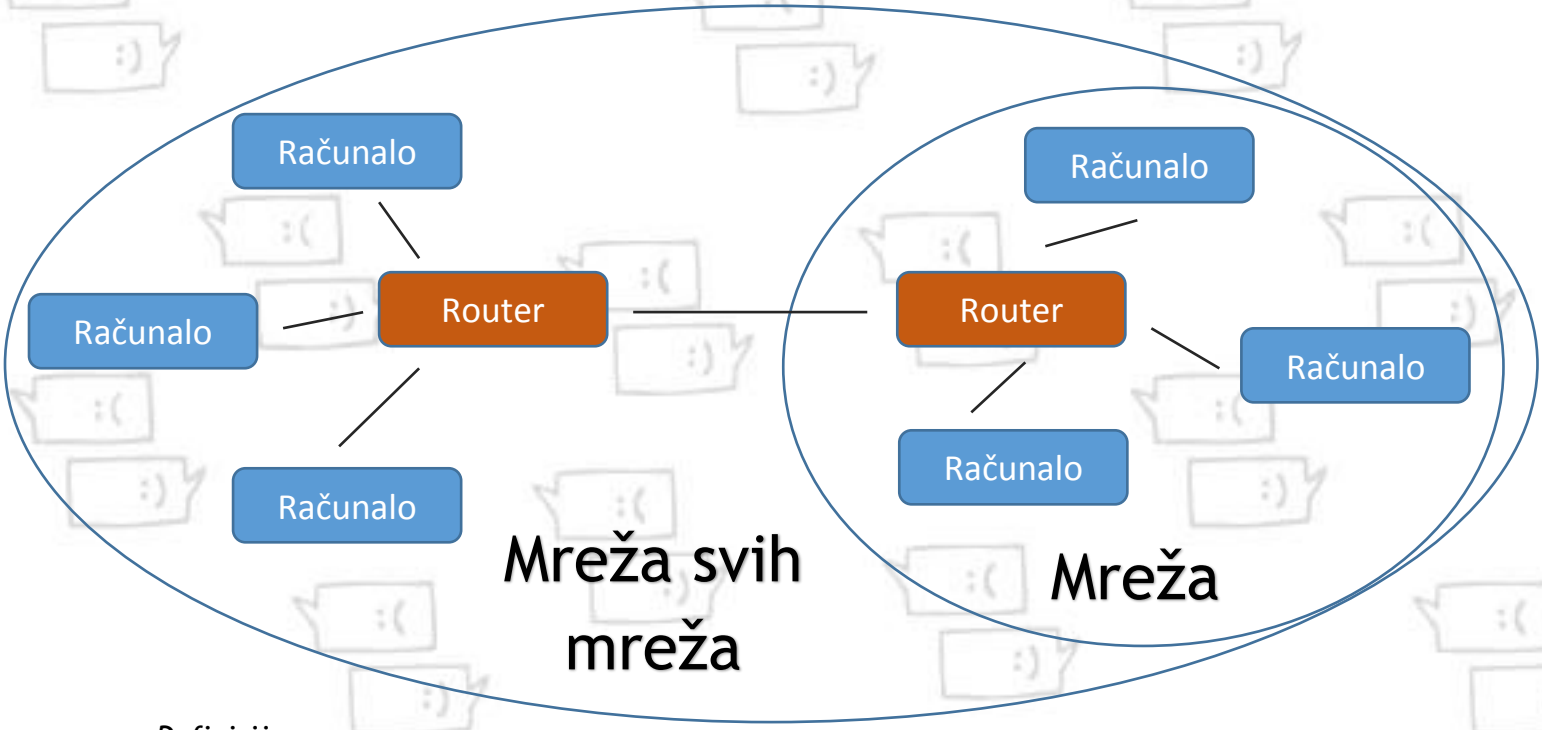
Zamolite učenike neka rade u grupama od 3 ili 4 i zabilježe dijagram interneta počevši od njihovog računala te odgovore na ova pitanja (5 minuta):

- Gdje su pohranjeni podaci koje dijelite na internetu? (Slike ili društvene mreže, članci na blogovima, video snimke na platformama za streaming...).
- Što znače ovi termini i kratice: hop, IP, packet, router, ISP i data server?

Zamolite dobrovoljce ili izaberite grupu koja će nacrtati svoj dijagram na ploči i izvijestiti razred o definicijama koje su pronašli. Zamolite ostale grupe da dopune/komentiraju dijagram i definicije (5 minuta)

Podijelite Dodatak 5 i pojasnite dijagram i definicije prema elementima prikazanima u nastavku (20 minuta).

Kad su dva i više računala povezana, ona tvore mrežu. Što je mreža veća, to su složenija "pravila" koja omogućuju njihovu komunikaciju (prijenos podataka). Internet je "mreža sastavljena od mnogo mreža" što zapravo znači da niz računala tvore mrežu i povezana su s drugim nizom računala koje tvore mrežu.



Definicije:

Hop (preskok) (u umrežavanju) je dio puta koji podaci prelaze od polazišta do odredišta (npr., "hop" je put između računala korisnika i ISP usmjernika, ili između ISP usmjernika i "backbone" usmjernika na internetu). Kako bi pristupili internetskoj stranici u Japanu, zahtjev korisnika za prikazivanje stranice i podaci koji se prenose natrag prema korisniku naprave puno "preskoka", a za svaki je potrebno nekoliko milisekunda.

- **IP** označava **"Internetski Protokol".** To je komunikacijski protokol koji omogućava dostavu paketa podataka od izvora do odredišta. Na primjer jedna od IP adresa Googlea je 74.125.224.72. Ako utipkate ova četiri broja u svoj pretraživač, prikazat će se početna stranica Googlea. No, s obzirom na to da IP adrese nije "praktično" pamtiti, ljudi koriste URL-ove (Uniform resource locator) ili web adrese koje odgovaraju IP adresi.
- **Paket** je formatirana jedinica podataka. Kako bi prenosili podatke putem interneta od internetske stranice do korisnika ili između dva korisnika (slike, video snimke, dokumente, internetske stranice), podaci se lome u manje dijelove koji se nazivaju "paketi". Paketi sadrže **kontrolne informacije i podatke o korisniku.** Kontrolne informacije su informacije koje pomažu mreži dostaviti podatke s jedne točke do

druge pri svakom **"hopu"** (poput adrese izvora, odredišta, otkrivanja pogrešnih kodova i informacija o tome kako pridružiti taj paket preostalim paketima i rekonstruirati podatke kad završi prijenos). Korisnički podaci su mali dio ukupnih podataka koji se šalje i prima.

- **Router (usmjernik)** je mrežni uređaj (specijalizirani hardver) koji prosljeđuje **pakete podataka** unutar računalnih mreža. Oni su ključni za osiguravanje sigurnog prijenosa vaših podataka na željeno odredište. Uređaj koji povezuje više računala u vašem domu također se naziva router jer prosljeđuje vaše pakete podataka između njih. Vrlo često, on ima i funkciju "modema", koji vas povezuje s vašim ISP-om i omogućuje vam pristup internetu. Vaš ISP, zauzvrat, prosljeđuje vaše pakete podataka putem puno sofisticiranijih routera sve dok podaci ne dođu na željeno odredište.
- **ISP** je skraćenica od **Internet Service Provider.** To je organizacija ili tvrtka koja pruža usluge koje vam omogućavaju pristup, korištenje ili sudjelovanje u Internetu. To je zapravo "glavni ulaz" za korisnike koji ulaze u internet.
- **Data center (centar podataka)** je prostor u kojem se nalazi velik broj računala koja se koriste u različite svrhe poput telekomunikacije ili pohrane podataka. To je također mjesto gdje se pohranjuje velika količina podataka s interneta (internetske stranice, datoteke..). Neke velike tvrtke poput Googlea, Microsofta ili Facebooka imaju vlastite data centre[7].

Pojednostavljena inačica interneta sastoji se od različitih "razina" (vidi prvu ilustraciju u Dodatku 5). Prvu razinu čine **korisnici,** pojedinci poput učenika i njihovih obitelji koji imaju uređaje koji se spajaju na internet putem fiksne linije (telefonske, kablovske TV..) ili bežične veze (mobilni podaci...). Ti korisnici povezuju se na **ISP** (internet service provider) koji im omogućava "ulaz" u "backbone" (središnji kanal) interneta (ključne, strateške točke koje omogućavaju međusobnu povezanost mreža). Puno njih prikazano je na **ilustraciji podvodnih kablova** u Dodatku 5. Većina podataka prenosi se s jednog kontinenta na drugi putem podvodnih kablova i na svakom kraju tih kablova nalaze se postrojenja s velikim brojem routera i ostalog hardvera koja omogućavaju prijenos podataka na željeno odredište. Nekad su svi podaci putovali fizičkim kablovima, ali danas, podaci se mogu slati i putem bežičnih mreža kao što su mobilni telefoni. Podaci koje šaljemo putem mobilnog telefona putuju prema "towerima" ili "baznim stanicama" mobilnih operatera i od tamo se preusmjeravaju na internet. Informacije se mogu prenositi i putem satelita.

Kako bi sve to funkcioniralo, internet se oslanjanja na brojna složena pravila. Jedna od njih je i **Internet Protocol (IP - internet protokol)** koji svakom uređaju spojenom na mrežu dodjeljuje jedinstveni broj (slično poštanskoj kućnoj adresi) kako bi podaci koji se šalju i primaju mogli naći svoje odredište. Podaci koji se prenose razlomljeni su u manje dijelove koje nazivamo "**paketi"** kako bi komunikacija bila učinkovitija. Umjesto slanja jedne velike datoteke u jednom neprekidnom signalu, podaci se šalju u manjim dijelovima putem kratkih izboja signala. To omogućava dvije stvari: gotovo simultano primanje i slanje raznih podataka (možete preuzeti datoteku dok gledate video) i povećava uspješnost komunikacije (ako paket ne uspije doći do odredišta, računalo na odredištu može poslati zahtjev da se ponovno pošalje samo taj paket umjesto da se ponovno šalju svi podaci).

[7] http://www.google.com/about/datacenters/inside/locations/index.html

Koje su implikacije? Zbog čega je važno znati kako funkcionira internet?

Zatražite učenike da razmisle o ta dva pitanja (2 minute) i neka dobrovoljci ili učenici koje ste vi izabrali iznesu svoja razmišljanja (3 minute).

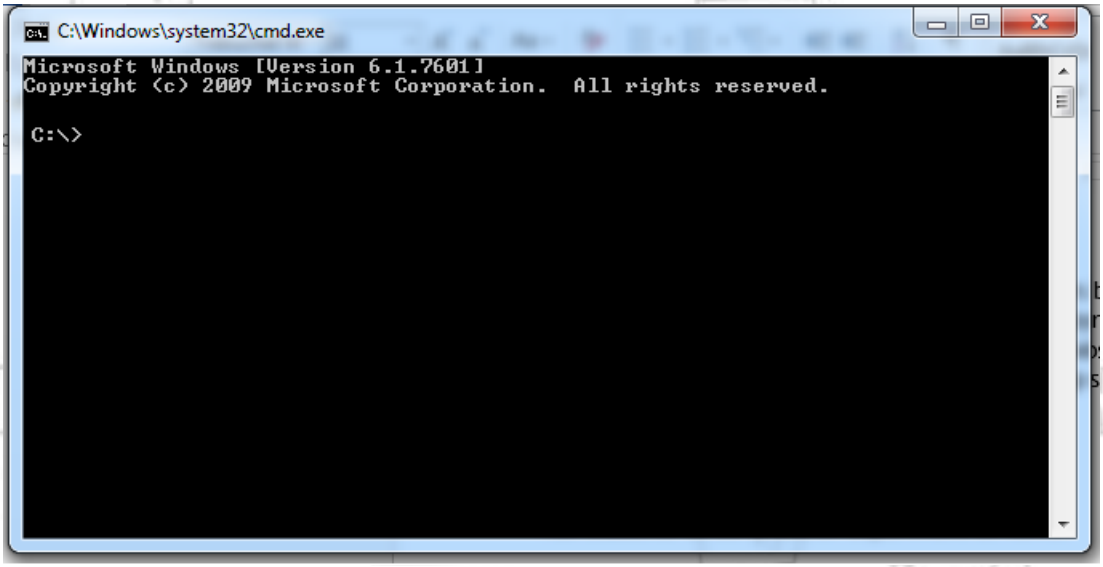
Iznesite neke od podataka iz nastavka (5 minuta):

- S obzirom na to da je internet decentraliziran i nijedna država nema punu kontrolu nad informacijama ili podacima (tekstovima, slikama, video materijalom, dokumentima...) koje šaljete internetom, ti podaci mogu izmaći Vašoj kontroli. Uzrečica "**jednom na internetu uvijek na internetu**" u sebi ima puno istine, pogotovo kada povezivač (vanjska osoba) ima pristup tim podacima i objavama s nekog drugog mjesta. Podaci koje šaljete u većini slučajeva su smješteni u stranoj državi i uklanjanje vaših podataka može biti vrlo težak ako ne i nemoguć zadatak. U EU, izmijenjena i dopunjena Direktiva o zaštiti osobnih podataka daje vam "pravo na zaborav" putem slanja zahtjeva pretraživačima da uklone vaše ime iz tražilice. Ali to ne znači da će podaci biti izbrisani, to samo znači da ih se neće moći pronaći korištenjem određene tražilice poput Googlea ili Binga.
- Kad tažite ili šaljete podatke putem interneta, podaci putuju preko određenih točaka. Na svakoj točki postoji **mogućnost sigurnosnog proboja i ugrožavanja podataka** (špijuniranja, gubitka, krađe, itd.) Nedavno otkriće **Edwarda Snowdena** pokazalo je da države mogu špijunirati internet kontrolom tih točaka na mreži poput kopnenih stanica koje obrađuju komunikacijske podatke koji putuju podvodnim kablovima. Ranjivost postoji i u bežičnim mrežama putem mobilnih uređaja i WiFi routera. Na primjer, ako se povežete na "public wifi" mrežu (javnu wi fi mrežu na aerodromu, kolodvoru...) i ne vodite računa je li vam veza osigurana, podaci koje šaljete i primate moći će biti "sniffed" (njuškani) ili "analysed" (analizirani) od ljudi koji su spojeni na isti WiFi router. Virusi i zlonamjerni programi također mogu kompromitirati vaš uređaj, omogućavanjem pristupa vašim podacima s udaljenog mjesta dokle god je vaš uređaj spojen na internet. Napokon, velik broj aplikacija sada su spojene na internet 24 sata dnevno, na mobilnim uređajima: facebook, whatsapp, skype, e-pošta, google now... i svi oni "osluškuju" svaki podatak koji bi im mogao biti namijenjen poput poruke ili obavijesti. Te stalne veze mogu biti ranjive i omogućiti eksploataciju ili kompromitiranje vašeg uređaja i podataka. Zbog toga je važno uvijek ažurirati software.
- Način na koji je internet oblikovan također znači da **nitko ne može biti 100% siguran da će ostati anoniman.** Policija, uz primjerenu potporu pravosuđa (sudski nalog), može istraživati i identificirati korisnike koji krše zakon na internetu. To uključuje i one koji se bave cyberbullyingom, kršenjem autorskih prava, itd. Mnogo je načina na koje se može otkriti tko stoji iza nekog posta. Internetske stranice bilježe IP adrese svih koji stupe u kontakt s njom. ISP također bilježi i čuva neke podatke koji se prenose putem vaše internet veze.

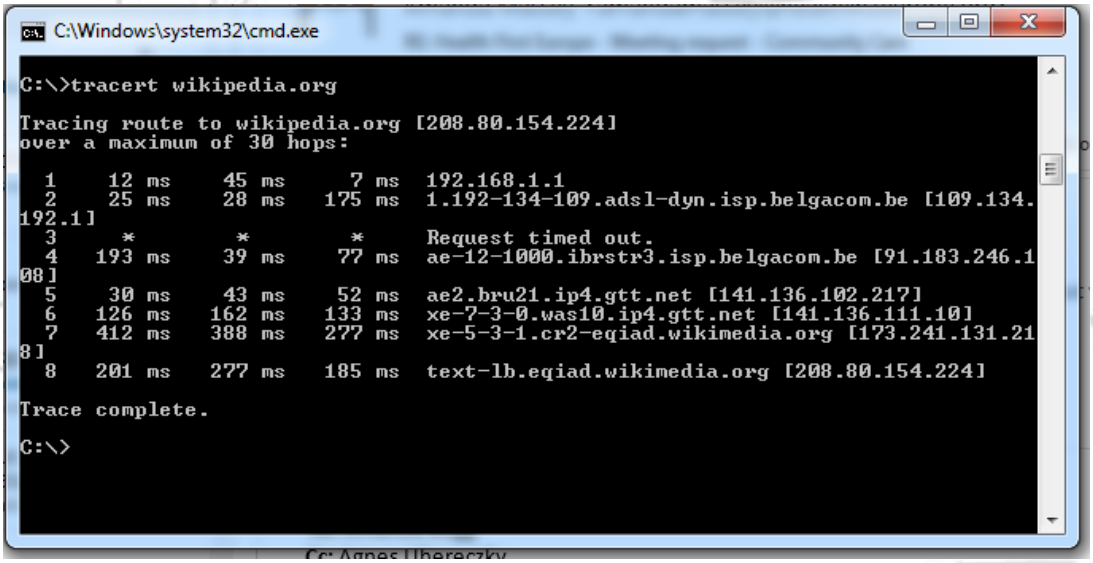
Dodatna aktivnost koju učenici mogu isprobati kod kuće:

Na Windows 7 ili novijoj inačici:

1) Kliknite na "start" gumb u Windowsima.
2) Ukucajte “cmd” u tražilicu i kliknite na programsku ikonu koja se pojavi na start meniju.



3) Ukucajte “tracert wikipedia.org” i pritisnite "enter".
4) Nakon toga ćete moći vidjeti "preskoke" (hops) između vašeg računala i internetske stranice kojoj pokušavate pristupiti i koliko vremena treba za svaki preskok. Na tom primjeru vidimo kako pristup Wikipediji, prvo ide preko routera vašeg "lokalnog ISP-a (u ovom slučaju Belgacom iz Belgije), zatim preko Atlanskog oceana do routera u Washingtonu (skraćenica "was"), i napokon stiže do mjesta gdje je smještena Wikipedija. Učenici naravno mogu to isprobati i s drugim stranicama.



Na Mac OS X i novijim inačicama:

1) Pokrenite network utility na Mac OS X (to možete učiniti ako odete na Spotlight i ukucate "Network Utility" i kliknete na prvi rezultat pretraživanja.
2) Kliknite na "Traceroute".
3) Unesite naziv domene kojoj želite pratiti rutu npr "Wikipedia.org" i kliknite Trace.
4) Nakon toga ćete moći vidjeti "preskoke" (hops) između vašeg računala i internetske stranice kojoj pokušavate pristupiti i koliko vremena treba za svaki preskok.

Dodatni izborni materijal za učitelja: https://www.youtube.com/watch?v=oj7A2YDgIWE

Aktivnost 7: Internet *spam*, *scam* i oglašavanje

Pitanje iz aplikacije: pitanje 9,16, 24, 25 i 30 iz kviza "Provjeri svoje znanje".

Trajanje: 50 minuta.

Dobna skupina: 14-18.

Domaća zadaća: prije sata zamolite učenike da istraže poslovne modele usluga koje najviše koriste na internetu (kako te usluge zarađuju novac). Vidi dolje za detalje.

Priprema: nema.

Slične aktivnosti: aktivnosti 5 i 6.

Ciljevi: razumjeti komercijalnu korist iza interneta i kako utječe na korisničko iskustvo na internetu.

Domaća zadaća:

U pripremi za sat, zatražite učenike da se podijele u parove ili skupine od 3-4 i kod kuće provedu malo istraživanje. Ohrabrite ih na korištenje suradničkih platformi poput Dropboxa, Google Drivea, One Drive, itd. Svaka grupa predstavit će poslovni model jednog od sljedećih servisa/igara/pružatelja sadržaja na internetu:

- Wikipedia
- Facebook
- Google
- Netflix
- World of Warcraft
- League of Legends
- Instagram/Whatsapp

Dodatni izbor ako su svi gore navedeni već dodijeljeni:

- Amazon
- Youtube

Njihovo istraživanje mora odgovoriti na sljedeća pitanja:

- Koji je glavni izvor prihoda (poslovni model) ovih usluga?
- Koje različite načine plaćanja osim plaćanja u gotovini koriste (kreditne kartice, debitne kartice...)?
- Kako, po vama, bi ti poslovni modeli i načini plaćanja mogli utjecati na krajnji proizvod/uslugu/sadržaj i vaše iskustvo kao korisnika?
    - *Na primjer, ako se internetska stranica oslanja na oglašavanje, to utječe na izgled stranice jer mora predvidjeti mjesto za reklamu. To također može utjecati i na čitljivost i privlačnost stranice za korisnike poput vas.*

Nastavni sat:

Na satu, zatražite sve skupine da prezentiraju svoje odgovore na prvo pitanje (2 minute po svakoj grupi, sveukupno 10-15 minuta).

U slučaju da učenici nisu pokrili te aspekte, nadopunite prezentacije učenika (prednosti i nedostaci biti će korisni za sljedeću aktivnost) informacijama navedenim u nastavku:

- Wikipedia: Poslovni model oslanja se na donacije.
    - Prednosti: oslanja se na dobru stranu ljudi, ne ovisi o privatnim interesima, nije pretrpana reklamama.
    - Nedostaci: ne može garantirati stabilan priljev prihoda i dugoročnu financijsku održivost, možda će trebati pribjeći oglašavanju kako bi prikupili donacije koje će možda biti jednako napadne kao i obično oglašavanje.
- Facebook: Poslovni model oslanja se na oglašavanje u najvećoj mjeri i plaćanjima Facebook igara/aplikacija, itd.
    - Prednosti: osigurava sve veći priljev prihoda (u skladu sa sadašnjim trendovima), korisnici ne trebaju plaćati pretplatu za korištenje usluge (oni plaćaju svojim osobnim podacima i vremenom koje potroše na gledanje/interakciji/klikanje na reklame).
    - Nedostaci: ovisi o trajnoj i ogromnoj bazi korisnika i stoga se mora agresivno nadmetati s konkurencijom poput drugih društvenih mreža (kad bi ljudi prestali koristiti Facebook, prihod od oglašavanja bi se urušio), postoji zabrinutost oko privatnosti i zaštite podataka. Javljaju se teškoće oko balansiranja sadržaja koji generiraju korisnici i potrebe za oglašavanjem (previše oglasa može odvratiti ljude, premalo može ugroziti prihode), to dovodi do rizika od prevelike manipulacije društvenim interakcijama između ljudi umjesto da osiguraju neutralnost i vidljivost vijesti (manipuliranje newsfeedom) u svrhu optimizacije prihoda. Trajno ulaganje napora kako bi se osiguralo da korisnici ostanu što duže na Facebooku jer što duže ostanu, to više raste prihod koji Facebook može zaraditi od reklama (postoji izravni interes da ljudi provedu što više vremena na Facebooku. To vrijedi i za korisničko sudjelovanje: što više podataka korisnici dijele na Facebooku to će više biti ciljani reklamama.)
- Google Poslovni model uglavnom se oslanja na reklame i nešto prihoda od prodaje proizvoda/usluga (poput Google smartphonea ili Google naočala, pružanja internetskih usluga, i sl.)
    - Prednosti: osigurava sve veći priljev prihoda (u skladu sa sadašnjim trendovima), korisnici ne trebaju plaćati pretplatu za korištenje usluge (oni

plaćaju svojim osobnim podacima i vremenom koje potroše na gledanje/interakciji/klikanje na reklame).
    - Nedostaci: ovisi o trajnoj i masivnoj bazi korisnika i stoga mora agresivno rješavati konkurenciju poput drugih društvenih mreža (kad bi ljudi prestali koristiti Google proizvode i usluge, prihod od oglašavanja bi se urušio), postoji zabrinutost oko privatnosti i zaštite podataka. Javljaju se teškoće oko balansiranja sadržaja koji generiraju korisnici i potrebe za oglašavanjem (previše oglasa može odvratiti ljude, premalo može ugroziti prihode), a to dovodi do rizika od prevelike manipulacije rezultatima pretraživanja ili newsfeedom kako bi optimizirali prihode umjesto da osiguraju neutralnost prikazanog sadržaja u tražilici kao i na svojoj društvenoj mreži. Trajno ulaganje napora kako bi se osiguralo da korisnici ostanu što duže na Googleu jer što duže ostanu, to više raste prihod koji Google može zaraditi od reklama (Google je već bio optužen za integraciju svih Google usluga poput tražilice, Google Maps, You Tube, Gmail, itd. u Google + vršeći pritisak na korisnike da se priključe na G+ i provode više vremena na njemu. Isto vrijedi za sudjelovanje korisnika: što više korisnika pretražuje uporabom Googlea, šalje e-poštu putem Gmaila ili dijele podatke na Google +, to će ih se bolje ciljati reklamama).
- Netflix: Poslovni model oslanja se na mjesečnu pretplatu.
    - Prednosti: korisnicima je lako razumljiva, osigurava stabilan i predvidljiv prihod, nema oglašavanja ili zlouporabe osobnih podataka.
    - Nedostaci: korisnici plaćaju uvijek isti iznos, bez obzira na intenzitet korištenja što ih može "pritisnuti" na "maksimiziranje" onoga što plaćaju (neki korisnici osjećaju obvezu koristiti uslugu samo zato da bi iskoristili ono što su platili), drugi konkurentski poslovni modeli poput "freemium" ili "besplatno uz oglašavanje" mogu im oduzeti bazu klijenata.
- World of Warcraft: Poslovni model oslanja se na mjesečnu pretplatu.
    - Prednosti: korisnicima je lako razumljiva, osigurava stabilan i predvidljiv prihod, nema oglašavanja ili zlouporabe osobnih podataka (iako to uvelike ovisi o igri: World of Warcraft smješten je u "fantasy" svijetu, i puno je teže integrirati oglašavanje. Neke online igre koje se odvijaju u "stvarnom svijetu" gdje su reklame bile dio igre kao dio dekora.)
    - Nedostaci: korisnici plaćaju uvijek isti iznos, bez obzira na intenzitet korištenja što ih može "pritisnuti" na "maksimiziranje" onoga što plaćaju (neki korisnici osjećaju obvezu koristiti uslugu samo zato da bi iskoristili ono što su platili), drugi konkurentski poslovni modeli poput "freemium" ili "besplatno uz oglašavanje" mogu im oduzeti bazu klijenata.
- League of Legends: Poslovni model oslanja se na "free-to-play" ili "freemium" poslovni model. Igranje je besplatno, no pristup dodatnim sadržajima koji omogućavaju brže napredovanje u igri se dodatno plaća.
    - Prednosti: korisnici plaćaju proporcionalno svojim potrebama (redovitiji korisnici plaćati će više od onih koji igraju samo povremeno), korisnici mogu isprobati igru/uslugu/sadržaj besplatno prije nego išta plate.
    - Nedostaci: postoji rizik stagnacije jer nema stabilnog, redovitog prihoda i manji je poticaj za unaprjeđivanje sadržaja/igre/usluge, ravnotežu između besplatnih i plaćenih sadržaja je vrlo teško pronaći (ako je previše toga besplatno nema nikakvog poticaja na kupnju što dovodi do izostanka

prihoda, ako je premalo toga besplatno, korisnici će možda odustati od igranja/korištenja usluge i pristupa sadržaju).

- Instagram/Whatsapp: To nije tipičan poslovni model već više "strategija" koja se naziva "build to sell" (izgradi i prodaj). Oslanja se na omogućavanje besplatnog korištenja softvera/usluge/sadržaja i izgrađivanje korisničke baze u nadi da će se putem naći neki poslovni model (npr. oglašavanje zbog porasta broja korisnika) ili da ćete uslugu prodati nekoj velikoj tvrtci kad postane popularna i stekne ogromnu korisničku bazu.
    - Prednosti: nema potrebe brinuti oko novca na početku "projekta" pa će usluga brzo biti dostupna, softver/usluga/sadržaj je za korisnike besplatan.
    - Nedostaci: nema jamstva da će softver/usluga/sadržaj moći financijski preživjeti i možda nestane nakon nekog vremena, nakon pronalaska poslovnog modela ili prodaje velikoj tvrtci (I Instagram i Whatsapp je kupio Facebook) softver/usluga/sadržaj može doživjeti značajne promjene i udaljiti postojeće korisnike (na primjer s pretjeranim oglašavanjem, promjenom dizajna ili funkcionalnosti, uvođenja sustava naplate..)
- Amazon: Poslovni model isti je kao bilo kojeg maloprodajnog lanca poput Konzuma, Interspara ili drugih. To je posao s fiksnim troškovima koji koristi internet za izvlačenje maksimuma iz nekretnina (skladišta i dostavnih centara): prodajom velike količine robe, može nadići fiksne troškove i stvoriti profit.
- Youtube: Poslovni model koji se oslanja na oglašavanje (video oglasi prije emitiranja željenog videa).

Općenita napomena: Ne postoji nijedan poslovni model koji jamči da će sve informacije i sadržaj na web stranici ili usluzi biti visoke kvalitete i pouzdanosti. Pouzdanost sadržaja na internetu može se mjeriti jedino internom politikom i identitetom/vlasništvom web stranice (ocjenjivanje sadržaja, citiranje, u vlasništvu akademske ustanove s reputacijom, itd.) a ne prema poslovnom modelu.

Online i ostale metode digitalnog plaćanja:

- Online usluge za prijenos novca poput PayPala.
- Virtualni online računi poput Google Wallet, Amazon Payments,...
- Globalna virtualna valuta poput Bitcoina ili lokalna virtualna valuta kao one iz online igara poput valute u League of Legends.
- Kreditne kartice (MasterCard, Visa.. sa ili bez sigurnosnog tokena).
- Debitne kartice (putem e-bankarstva i sigurnosnog tokena)
- NFC (Near Field Communication): ova tehnologija omogućava plaćanje putem smartphonea ili kreditnih kartica s NFC-om jednostavno prislanjanjem uređaja ili kartice na prijemnik.
- Mobilno plaćanje: uključuje sve moguće načine na koje netko može platiti mobitelom poput premium SMS usluga, izravne naplate operatera (troškovi se dodaju na vaš račun za telefon), online novčanici, itd.
- Podaci: zanimljivo je da su podaci o korisnicima koji omogućavaju prilagodbu ponude oglašavanja postali novi oblik online valute .

Upitajte razred koji poslovni model, po njihovom mišljenju je najučestaliji i najpopularniji (5 minuta rasprave).

Podijelite Dodatak 6 i zamolite učenike da ga pregledaju i prepoznaju ključne riječi. Zamolite grupe da iznesu svoja mišljenja (5 minuta).

Ako učenici nisu naglasili sljedeće trendove vi ih iznesite:

- Prihod od oglašavanja većine online servisa raste što znači da rastu i troškovi oglašavanja (koliko tvrtke plaćaju za online marketing).
- Sve je popularniji i prošireniji model "freemium"

Pitajte učenike što misle zašto su "freemium" i "free-to-play" i modeli oglašavanja najuspješniji i zapišite na ploču njihove odgovore, nadopunjavajući njihove odgovore elementima prikazanima gore (prednosti i nedostaci) i dolje (sažetak uzroka). (5 minuta)

- Uspjeh "Freemium" ili "free-to-play" modela proizlazi iz sljedećih koristi za korisnika:
    - "besplatan" je do određene razine,
    - korisnici ga mogu isprobati prije nego što išta plate,
    - strastveni igrači mogu platiti premium usluge a povremeni korisnici mogu se držati besplatne inačice.
    - korisnici mogu nadograditi i platiti kadgod žele.
- Uspjeh modela oglašavanja leži u činjenici da ga korisnici percipiraju kao "besplatni" i ne razumiju koju "cijenu" plaćaju za softver/uslugu/sadržaj (eksploatacija njihovih osobnih podataka kako bi ih se bolje ciljalo oglasima).

Pitajte učenike da razmisle o tome kako ti poslovni modeli utječu na softver/usluge/sadržaj koje oni koriste (neka se posluže svojim zaključcima iz domaće zadaće); nadopunite njihove odgovore elementima prikazanima u nastavku (10 minuta).

- "Freemium" ili "Free-to-play" modeli mogu imati sljedeći utjecaj:
    - Softver/usluga/sadržaj koji koristite oblikovan je kako bi izazvao ovisnost i koristi se kako bi osigurao da korisnici ulože novac u premium značajke. Na primjer, u ključnim trenucima tijekom igre, korisnik će morati platiti premium sadržaj da bi napredovao.
- Modeli "oglašavanja" mogu imati sljedeći utjecaj:
    - Pokušavaju postići da produže vrijeme koje provodite koristeći njihov softver/uslugu/sadržaj kako bi povećali prihod. To podrazumijeva pokušaj pridobivanja pozornosti korisnika i njihovo zadržavanje na primjer na nekoj web stranici što je duže moguće. Utjecaj na korisnika znači da čitave web stranice očajnički pokušavaju trošiti vaše vrijeme kako bi maksimizirali svoj profit od oglašavanja. Taj termin naziva se "stickiness" (ljepljivost) u žargonu online oglašavanja.
    - S nastankom ciljanog oglašavanja, online servisi poput društvenih mreža postale su zainteresirane za to da ljudi dijele što više informacija o svojim životima. Oglašivači kupuju oglasni prostor na društvenoj mreži i oslanjanju se na pretpostavku da je njihov novac uložen znatno učinkovitije nego u klasičan oglas jer mogu precizno odrediti tko će vidjeti taj oglas, filtrirajući publiku po dobi, spolu, lokaciji, jeziku/državi, razini obrazovanja i raznim drugim informacijama (glazba/filmovi koje volite, hobiji, itd.)
    - Prisutnost privatnih tvrtki na društvenim mrežama i ostali servisi oslanjaju se na oglašavanje za stjecanje prihoda znači da bilo koji korisnik može postati agent za oglašavanje neke privatne tvrtke. Na primjer, ako lajkate neki brend na Facebooku, to će tvrtki dati pravo prikazivanja oglasa svim vašim prijateljima time što ste ih obavijestili da vam se sviđa njihova tvrtka/proizvod. Na You Tubeu na primjer, korisnici mogu zarađivati uključujući video oglas prije projekcije njihovog videa, što također pretvara korisnike YouTubea u oglašivače. To stvara snažan poticaj da povećate

gledanost i dostignete stupanj "virala" pod svaku cijenu (nauštrb kvalitete sadržaja na primjer, postavljanje smiješnog/blesavog sadržaja je privlačnije od obrazovnog). Ono što još više uznemirava je činjenica da korisnike koji stavljaju video snimke ili blog postove na internet i imaju veliku gledanost kontaktiraju tvrtke i navode ih da izravno spominju ili prikazuju proizvode ili brendove u svom sadržaju.

- Da sažmemo, najuspješnije reklamne kampanje su one koje osiguravaju angažman i interakciju korisnika, njihove komentare, lajkanje, dijeljenje oglasa ili proizvoda. Primjer takve strategije je Coca-Colina "Share a coke" (Podijeli Coca Colu) kampanja, u kojoj su sami korisnici bili uključeni u postanje fotografija boca Coca Cole sa svojim imenima i imenima svojih prijatelja, i tako služili kao širitelji kampanje, a da to Coca Colu nije koštalo ništa. (Vidi Dodatak 7 s primjerima)

Zatražite učenike da razmisle o tome kako sve veći broj načina plaćanja na internetu utječe na njihovo online okruženje, pogotovo vezano uz spam i scam i nadopunite njihove odgovore elementima prikazanima u nastavku (10 minuta).

- Uz rastući broj novih načina plaćanja, jednako raste i broj načina "izvlačenja" novaca od korisnika interneta, bilo na zakonit ili nezakonit način. To također uključuje izvlačenje podataka i informacija od korisnika (poput profila društvenih mreža, postova, sadržaja e-pošte, pretraživanja ključnih riječi, čak i geolokacije).
  - *Oglašavanje:* zakonito, kao što su pokazali trendovi o kojima smo govorili ranije (rastuća e-prodaja i investiranje u internetski marketing), snažno se potiče oglašavanje usmjereno prema korisnicima interneta s obzirom na to da je on-line kupnja postala lakša nego ikad prije.
  - *Spam:* na granici između zakonitog i nezakonitog , velika količina spama je ili prenametljivo oglašavanje ili jednostavno "scam" (prevara). Termin se uglavnom koristi za neovlašteno slanje e-poruka zagađivanjem računa e-pošte, ali se može i proširiti na postove ili pozive na društvene mreže, komentare na videa, blogove, itd.
  - *Scam:* nezakoniti pokušaji prevare korisnika i navođenje na trošenje novaca ili kompromitiranje korisnikovih podataka (društvene mreže, računi e-pošte). S obzirom na to da je plaćanje putem interneta olakšano to je utjecalo i na porast ove pojave tijekom godina. (Primjer se može naći u Dodatku 7, u kojem korisnici trebaju unijeti svoj broj telefona kako bi osvojili iPad, što rezultira pretplatom na premium SMS uslugu koja skida novac s njihove kartice mobitela).
- Zaključno, olakšano plaćanje putem interneta i nove valute poput korisničkih podataka potaknule su rast oglašavanja, *spama* i *scama*. Korisničko iskustvo vezano uz okruženje na internetu takvo je da korisnik ne raspoznaje razliku između, oglasa, spama i scama zbog njihove sve veće prisutnosti. Na primjer, pokušaj krađe lozinke za ulazak u e-poštu ili račun na društvenoj mreži (phishing) postaje sve teže uočljiv: e-pošta koju prima korisnik izgleda kao "prava" e-pošta koja stiže od pružatelja usluga neke društvene mreže. Puno se radi i na tome da se korisnici navedu na klikanje koje ih vodi na oglas/spam/scam umjesto na sadržaj kojem su htjeli pristupiti putem neprimjetnog spajanja oglasa/spamova/scamova sa sadržajem (na primjer stvaranjem velikog gumba za "download" /preuzimanje/ koji vas preusmjeravaju na drugi sadržaj i manje uočljiv za stvarno preuzimanje datoteke koju ste tražili).

<u>Kakve to ima veze sa cyberbullyingom?</u>

Cyberbullying je uglavnom problem vezan uz ponašanje i ljude, ali omogućuje ga tehnologija. Cyberbullying se događa na mnogo online platformi, servisa, web stranica, igara, uređaja... i način na koji su oni konfigurirani, njihove interne politike, zadane postavke, značajke zaštite privatnosti i poslovni modeli mogu ponekad pogoršati ili olakšati cyberbullying.

Na primjer, mnogo usluga uključujući i društvene mreže oslanjaju se na razne elemente kako bi ostvarivale prihod od oglašavanja. Među njima je i **maksimiziranje korisničkog sudjelovanja** (dijeljenje, komentiranje, postanje, interakcije, linkanje, itd.) jer će im to omogućiti prodaju detaljnijih informacija o njihovim korisnicima oglašivačima i stoga povećati učinak njihovih reklamnih kampanja, koje će ciljati na vrlo specifične korisnike temeljem velike količine podataka i informacija koje generiraju. To također znači da te usluge imaju interes u tome da **ljudi svoje profile drže otvorenima** (umjesto da svoj sadržaj u potpunosti zaključate, što bi značilo da će vaši postovi/aktivnosti biti vidljivi ograničenoj publici) i **da čuvaju što je više moguće podataka o korisnicima** (odvraćajući ih od toga da "očiste" svoje račune redovno ili izbrišu ogromnu količinu prošlih uključivanja i postova).

Lako je vidjeti da ti čimbenici mogu povećati vjerojatnost da netko postane žrtvom cyberbullyinga ili otežati blokiranje (otvaranje profila, manje kontrole nad vlastitim podacima...)

To je samo jedan primjer kako određeni poslovni model utječe na ishod ljudskog ponašanja.

DODATAK 1: POPIS PITANJA IZ APLIKACIJE

Pitanja u dijelu "Provjeri svoje znanje" (točni odgovori u boldu)

1) *Što je cyberbullying?*

- Slanje uvredljivih poruka.
- Silom uzeti nečiji mobitel i obrisati sve podatke prije vraćanja mobitela vlasniku.
- **Pokušati namjerno nekoga povrijediti uzastopnim slanjem uvredljivih poruka ili slika putem interneta .**
- Poslati elektroničku poštu svim svojim kontaktima i pokušati ih na prevaru nagovoriti da ti pošalju novac.
- Kada te kontaktira odrasla osoba koja ima zle namjere i koja te prisiljava da radiš stvari koje ne želiš raditi na internetu.

2) *Koliko je tvojih prijatelja iz razreda doživjelo cyberbullying?*

- Manje od jednog na dvadeset.
- Manje od jednog na deset.
- **Otprilike jedan od pet.**
- Jedan od dvoje (50%).

3) *Tvoj prijatelj ili prijateljica su doživjeli cyberbullying. Što misliš, koliko bi to moglo postati ozbiljno?*

- Ništa ozbiljno. Lako će to sami riješiti.
- **Može dovesti do depresije i samoozljeđivanja. Mogli bi se osjećati kao bespomoćne žrtve cyberbullyinga.**
- Neko kraće vrijeme može biti frustrirajuće, ali uvijek mogu obrisati ili ignorirati stvari koje ih smetaju.
- Može imati trajne posljedice na njihov ugled.

4) *Što trebaš napraviti ako dobiješ nekoliko negativnih komentara/postova ili prijetećih poruka?*

- Obrisati poruke i zaboraviti na to.
- Odmah odgovoriti istom mjerom i rječnikom.
- **Ne odgovoriti, sačuvati sve dokaze i razgovarati o tome s odraslom osobom ili prijateljem kojem vjerujem.**
- Podijeliti ih s prijateljima i kontaktima kako bi pokazao koliko je poruka loša.

5) *Ako primijetiš da netko stalno dobiva uznemiravajuće poruke trebao bi:*

- **Pomoći osobi koju uznemiravaju, razgovarati sa odraslom osobom od povjerenja i ako misliš da to možeš, zamoliti nasilnika da prestane.**
- Ne poduzeti ništa i držati se po strani kako ne bi i sam postao žrtvom uznemiravanja.
- Uzvratiti jednako uvredljivim porukama kako bi osoba na vlastitoj koži osjetila kako je to kada te uznemiravaju.
- Savjetovati osobi koju uznemiravaju da ne bude slabić i neka ne provocira nasilnike.

6) *Nasilje uživo je puno gore od cyberbullyinga.*

- Točno.
- **Netočno.**

7) *Što su seksi poruke (sexting)?*

- Dijeljenje slika na kojima si bez odjeće.
- Dijeljenje video snimaka na kojima si bez odjeće.
- Slanje teksta u kojem pišeš o seksu.
- **Sve navedeno.**

8) *Kako možeš provjeriti je li osoba s kojom komuniciraš online zaista ona koja misliš da jest?*

- Tražiš da ti pošalje kopiju osobne iskaznice.
- Tražiš da uključi kameru dok komunicira s tobom.
- Postaviš tajno pitanje na koje samo ta osoba može znati odgovor.
- **Nikada ne možeš znati sa sigurnošću.**

9) *Zašto ne možeš otvoriti profil na društvenoj mreži dok ne navršiš 13 godina?*

- Zato što su društvene mreže samo za odrasle.
- Na društvenim mrežama ima puno nasilnih, seksualnih ili šokantnih stvari.
- **Zakon zabranjuje korištenje osobnih informacija u komercijalne svrhe prije navršenih 13 godina.**
- Da bi se mogao pridružiti društvenoj mreži moraš barem minimalno poznavati jezik i informatiku.

10) *Kakve su posljedice ako se otkrije da si nad nekim vršio/la cyberbullying?*

- Nikakve, ako ostanem anoniman/na i nema dokaza.
  Kaznit će me roditelji ili učitelji.
- Pružatelj internetskih usluga će mi isključiti internet.
- **Pravne posljedice, imat ću problema s policijom.**

11) *Imaš li pravo objaviti slike svojih prijatelja na internetu?*

- Da, imam. Ako sam ih ja slikao, onda su to moje slike.
- **Ne, osim ako ne dobijem njihov pristanak.**
- Mogu objaviti slike, ali oni će odlučiti hoće li se označiti ili će maknuti oznaku (tag).
- Da, ako su se složili s time da ih slikam, onda ih mogu i objaviti.

12) *Ako označiš da ti se sviđa ili objaviš uvredljiv komentar ili sliku kojom si nekoga posramio, smatra li se to cyberbullyingom?*

- Ne, netko drugi ju je objavio.
- **Da, i to se može smatrati cyberbullyingom.**

13) Možeš li ostati anoniman na internetu?

- Da, ako si vješt s kompjuterima.
- Da, čak ako i nisi vješt s kompjuterima, možeš napraviti lažan nadimak/nickname ili profil.
- **Ne, nikad ne možeš biti siguran da ćeš ostati anoniman.**

14) Možeš li obrisati slike ili komentare jednom kada si ih objavio na internetu?

- Da, samo pritisneš delete.
- Da, osim ako ih je netko drugi ponovno objavio nakon tebe.
- Da, možeš zamoliti administratora društvene mreže (Facebook, Youtube) da obriše sve kopije tvojih objava ili slika.
- **Ne, nikada ne možeš biti siguran da su tvoje objave ili slike zauvijek obrisane s interneta.**

15) Jesu li poruke objavljene na servisu koji automatski briše poruke nakon određenog vremena (primjerice Snapchat) zasta obrisane?

- Da, tako je taj servis dizajniran.
- **Ne, sustav se može zaobići na puno načina.**

16) Koje od ovih metoda možeš koristiti za prepoznavanje pokušaja phishinga? (krađa identiteta putem interneta)

- Adresa e-pošte pošiljatelja je sumnjiva (npr. password@1.twiter.com umjesto password@twitter.com).
- Sadržaj e-pošte je sumnjiv (npr. položaj teksta, slova i slike u e-pošti izgledaju neobično).
- Traže da pošalješ podatke o računu (korisničko ime i lozinku...) direktno putem e-pošte.
- Preusmjere te na sumnjivu web stranicu (npr. www.1.twiter.com umjesto www.twitter.com).
- **Sve navedeno.**

17) Kome možeš povjeriti svoju lozinku?

- Najboljem prijatelju ili prijateljici.
- Potpuno nepoznatoj osobi.
- Bratu ili sestri.
- Svojem dečku ili djevojci.
- **Roditeljima.**
- Svojem učitelju ili učiteljici.

18) Kome možeš dati svoj broj mobitela?

- **Prijateljima i obitelji.**
- Učenicima iz razreda, prijateljima i obitelji.
- Svakome iz škole ili s posla, prijateljima i obitelji.
- Svakome tko ga zatraži, mogu ga čak i objaviti na internetu.

19) Što je najgore što se može dogoditi ako svoj broj mobitela javno objaviš?

- Mogu mi pristizati neugodne poruke ili telefonski pozivi od potpunih stranaca koje ću morati obrisati ili ignorirati.
- **Mogu mi pristizati neugodne i uvredljive poruke ili telefonski pozivi, čak bih mogao biti pretplaćen na usluge koje se naplaćuju (SMS usluge, ringtone melodije…).**
- Ništa, nije opasno javno objaviti svoj telefonski broj.
- Pristizat će mi reklame i pozivi od teleprodaje.

20) Kome možeš dati svoju kućnu adresu?

- **Prijateljima i obitelji.**
- Učenicima iz razreda, prijateljima i obitelji.
- Svakome iz škole ili sa posla, prijateljima i obitelji.
- Bilo kome, nije bitno, to nije povjerljiv podatak.

21) Što je najgore što se može dogoditi ako javno objaviš svoju kućnu adresu?

- Nepoznate osobe će me dolaziti posjetiti.
- Pristizat će mi neugodna pošta ili reklame.
- **Netko će me uznemiravati ili čak opljačkati dok sam s obitelji na praznicima.**
- Ništa, sigurno je javno objaviti svoju kućnu adresu.

22) Gdje su pohranjeni svi tvoji online podaci? (primjerice slike s praznika na društvenim mrežama)

- Negdje na hard disku mojeg kompjutera.
- **Na hard diskovima ogromnih skladišta koja se zovu "centri podataka" u različitim stranim državama.**
- Na hard disku pružatelja internetske usluge u mojoj državi.
- Na satelitima koji kruže oko Zemlje.

23) Koja je od ovih tvrdnji netočna? Važno je promisliti prije objavljivanja na internetu jer:

- Netko bi to mogao zloupotrijebiti i vršiti cyberbullying nad tobom.
- Može se dogoditi da ne dobiješ posao zbog objave neozbiljnog sadržaja.
- Može omogućiti lopovima da o tebi doznaju privatne podatke koji će im omogućiti da te opljačkaju.
- Oglašivači bi to mogli iskoristiti i nagovoriti te da kupuješ više stvari.
- Negativno će se odraziti na mišljenje drugih o tebi i na to koliko im se sviđaš ili ne sviđaš(možda nećeš biti popularan ili popularna).
- **Moglo bi oštetiti hard disk tvojeg kompjutera.**
- Na koji način većina "besplatnih" online servisa ili igara zarađuje novac?

24) Na koji način većina "besplatnih" online servisa ili igara zarađuje novac?

- Financira ih vlada (kroz poreze koje plaćaju građani).
- Dobivaju donacije.

- **Prodaju tvoje osobne podatke oglašivačima i objavljuju reklame.**
- Stvaraju ih jako bogati ljudi koji u njih ulažu vlastiti novac.
- Uopće ne zarađuju nego rade kao volonteri.

25) Koji se od ovih online servisa financira uglavnom kroz donacije?

- **Wikipedia (online enciklopedija).**
- Facebook (društvena mreža).
- Google (pretraživač).
- Yahoo! (e-pošta).
- Youtube/Dailymotion (servis za prikazivanje videa).

26) Koja je od ovih tvrdnji netočna? Sigurna lozinka:

- **Treba biti iz rječnika.**
- Treba sadržavati barem 8 znakova.
- Treba kombinirati slova, brojeve i simbole.
- Treba je redovito mijenjati.
- Treba biti jednaka za sve tvoje online račune.

27) Najveća je vjerojatnost da ćeš online upoznati strance s lošim namjerama:

- **Na otvorenim chat sobama ili aplikacijama.**
- Na društvenim mrežama.
- Na aplikacijama za instant poruke.
- Blogovima.

28) Što je od sljedećeg IP adresa?

- **192.0.81.250**
- www.deletecyberbullying.eu
- #DeleteCyberbullying
- @DeleteCyberbullying
- info@deletecyberbullying.eu

29) Koju od sljedećih informacija fotografija snimljena smartphone uređajem nikada ne sadržava?

- Veličinu slike.
- Datum i vrijeme kada je snimljena.
- Točnu GPS lokaciju na kojoj je snimljena.
- **Tvoj broj telefona.**
- Koji objektiv koristi kamera na tvom telefonu.

30) Važno je promisliti prije "lajkanja" neke Facebook stranice?

- Ne, to nije opasno. Mogu "lajkati" kolikogod stranica želim.
- **Da, ne treba vjerovati svim Facebook stranicama.**

Pitanja u dijelu "Jesi li ikad doživio/la?

1) *Razgovaraš li sa roditeljima o onome što radiš online?*

- Da, redovito razgovaram s njima.
- Da, ponekad.
- Da, razgovaram s njima o nekim stvarima koje radim online na internetu, ali ima stvari o kojima ne razgovaramo jer su previše osobne.
- Ne, nikada.

2) *Jesi li ikad prilikom prijave na svoj profil otkrio da ti se lozinka promijenila?*

- Da, dogodilo mi se nekoliko puta.
- Da, dogodilo mi se jednom ili dvaput.
- Ne, ali se dogodilo mojem prijatelju ili prijateljici.
- Ne, nikada.

3) *Jesi li ikada saznao da su neke tvoje tajne objavljene na internetu?*

- Da, dogodilo mi se nekoliko puta.
- Da, dogodilo mi se jednom ili dvaput.
- Ne, ali se dogodilo mojem prijatelju ili prijateljici.
- Ne, nikada.

4) *Jesi li ikada vidio neželjen materijal (slike, filmovi, objave) objavljen o sebi na internetu?*

- Da, dogodilo mi se nekoliko puta.
- Da, dogodilo mi se jednom ili dvaput.
- Ne, ali se dogodilo mojem prijatelju ili prijateljici.
- Ne, nikada.

5) *Moji prijatelji, dečko ili djevojka nagovorili su me na slanje seksi poruka (sexting - dijeljenje slika, filmova ili komentara seksualne prirode), a zatim su te slike podijelili s drugima.*

- Da, dogodilo mi se nekoliko puta.
- Da, dogodilo mi se jednom ili dvaput.
- Ne, ali se dogodilo mojem prijatelju ili prijateljici.
- Ne, nikada.

6) *Prijavili su te na natjecanje ili anketu (primjerice jesi li seksi ili nisi) bez tvojeg pristanka?*

- Da, dogodilo mi se nekoliko puta.
- Da, dogodilo mi se jednom ili dvaput.
- Ne, ali se dogodilo mojem prijatelju ili prijateljici.
- Ne, nikada.

7) *Jesi li ikada objavio sadržaj (slike, filmove, komentare, poruke) o nekome bez njihovog pristanka?*

- Da, nekoliko puta.
- Da, jednom ili dvaput.
- Neki od mojih prijatelja i prijateljica su to napravili.
- Ne, nikada.

8) *Jesi li se ikada predstavio kao da si netko od tvojih školskih prijatelja ili neka druga osoba?*

- Da, nekoliko puta.
- Da, jednom ili dvaput.
- Ne, nikada.

9) *Jesi li isključio nekoga iz grupe na internetu i jesu li tebe isključili iz grupe na internetu čiji si član želio biti?*

- Isključio sam nekoga iz grupe na internetu.
- Isključio sam neke osobe zbog njihovog lošeg ponašanja.
- Isključio me moderator.
- Isključili su me drugi redoviti članovi grupe.
- Isključio sam druge, ali i mene su isključivali.
- Vidio sam da se takve stvari događaju.
- Ništa od navedenog.

10) *Je li anonimnost na internetu prednost ili nedostatak?*

- Više je nedostatak jer su me ljudi anonimno vrijeđali i osjećao sam se bespomoćno.
- Više je prednost jer mogu raditi što god želim, čak i anonimno vrijeđati ljude.
- Više je prednost jer me anonimnost štiti od mnogih stvari uključujući i cyberbullying.
- Anonimnost može biti i dobra i loša. Ovisi o situaciji.
- Nemam mišljenje o ovom pitanju.

11) *Jesi li mijenjao nečije slike ili video snimke bez njihovog pristanka i objavljivao to na internetu?*

- Da, nekoliko puta.
- Da, jednom ili dvaput.
- Ne, nikada.

12) *Ako si ikada nekoga uznemiravao putem interneta, ili ako bi to učinio u budućnosti, zašto bi to učinio? (Više mogućih odgovora)*

- To nije ništa ozbiljno, to je samo šala.
- Učinio sam to iz osvete.
- Svi to rade, samo sam se pridružio.
- Bio sam ljut ili uzrujan zbog nečega.
- Morao sam, inače bi me odbacili ili bih bio iduća meta.
- Bilo mi je dosadno.
- Lakše je nego fizičko nasilje i mogu ostati anoniman.
- Drugi razlozi.
- Nikada ne bih ni nad kim vršio cyberbullying.

DODATAK 2:

Kazneni zakon i internet

infinius.hr/blog/kazneni-zakon-i-internet/

S početkom ove, 2013 godine, su se dogodile značajne promjene u Hrvatskoj vezane uz zakon i to naročito što se tiče kažnjivih djela na internetu. Naime, još prije više od godinu dana, točnije 21. listopada 2011 je izglasan novi Kazneni zakon koji u velikoj mjeri uključuje i ponašanje na računalnim sustavima i mrežama – što uključuje internet te društvene mreže.

Uvreda, sramoćenje i kleveta

Tako je za kazneno djelo uvrede, ukoliko je ono počinjeno javno putem interneta tj. uvreda je postala pristupačna većem broju osoba, u novom zakonu predviđena novčana kazna do sto osamdeset dnevnih iznosa (gdje se dnevni iznos utvrđuje uzimajući u obzir počiniteljeve prihode i imovinu – a ne može biti manji od dvadeset kuna ni veći od deset tisuća kuna).

Sramoćenje (iznošenje ili prenošenje činjeničnih tvrdnji koje mogu škoditi časti ili ugledu neke osobe) putem interneta vas također može dosta osiromašiti – čak do tri stotine i šezdeset dnevnih iznosa (tj. godišnjeg prihoda), no ovo vrijedi samo za neistinite tvrdnje – ukoliko možete dokazati istinitost

tvrdnje kaznenog djela nema. Ako se svjesno iznosi neistina koja može škoditi nečijem ugledu, riječ je o kleveti te su moguće i veće kazne.

Govor mržnje

Za poticanje na nasilje i mržnju putem interneta se može očekivati do tri godine zatvora (ovo vrijedi i za one koji isto javno odobravaju), dok organizatori ili oni koji vode grupu više od tri osobe mogu očekivati još strože kazne.

Ovo se naročito odnosi na pozivanje na mržnju prema skupini ili njihovim pripadnicima zbog njihovih osobina (rasne, vjerske, nacionalne ili etičke pripadnosti te spolnog opredjeljenja i ostalog), no i na poricanje kaznenog djela genocida, agresija te zločina protiv čovječnosti ili ratnog zločina.

Zakon i djela protiv računalnih sustava – hakiranje

Osim ovih javnih istupa protiv drugih osoba na internetu, čak cijela glava Kaznenog zakona je posvećena kaznenim djelima protiv računalnih sustava, programa i podataka (popularno "hakiranje") te su tako predviđene zatvorske kazne do osam godina zatvora.

Neovlašteni pristup računalnom sustavu ili podacima se kažnjava do jedne godine zatvora, osim u slučaju računalnih sustava i podataka državnih vlasti gdje je moguća kazna do tri godine (kažnjava se i sami pokušaj, stoga pazite što radite!). Ometanje računalnih sustava – DoS, DDoS i slični napadi se po zakonu kažnjavaju kaznom zatvora do tri godine, jednako kao i za oštećenje računalnih podataka ili programa.

Kažnjivo je i presretanje te snimanje nejavnih podataka i prijenos trećim osobama, stoga ukoliko npr. čitate ili čak prenosite nekome drugome e-mail koji nije namijenjen vama – računajte da je za ovo moguća kazna zatvora do tri godine. Ukoliko je riječ o računalnoj prevari s ciljem da se sebi ili drugome pribavi protupravna imovinska korist, minimalna kazna zatvora je šest mjeseci – a u slučaju značajnih iznosa do čak osam godina zatvora. Kažnjivo je također i posjedovanje, kao i izrada ili prodaja uređaja i programa (skripte i slično) koji omogućavaju navedena kaznena djela, a isto vrijedi za lozinke.

Teškim kaznenim djelima se smatraju ona djela koja se provode protiv računalnih sustava državne vlasti ili javnih ustanova, ali i za napade na veći broj računalnih sustava ili prouzrokovanje znatne štete uslijed kaznenih djela, no još značajnije – i ona djela koja su počinjena prikrivajući stvarni identitet…

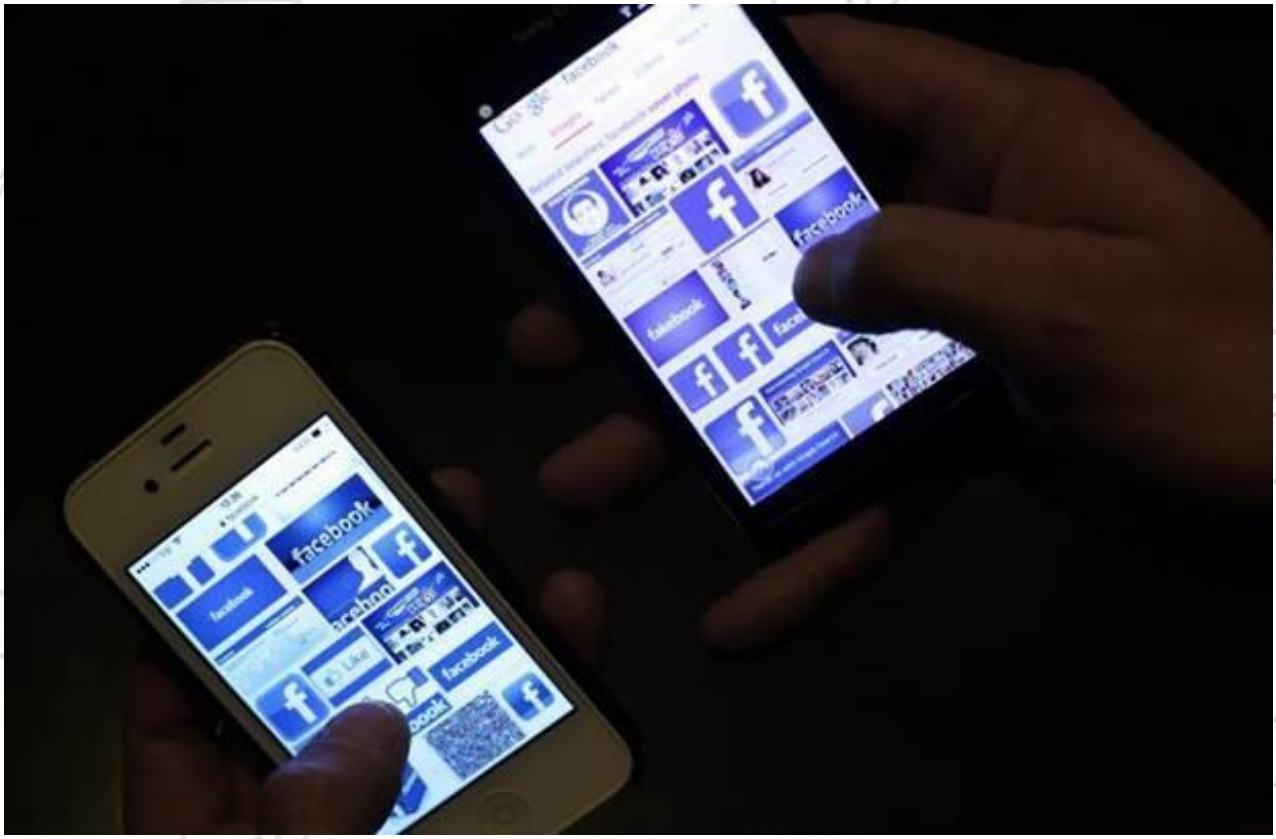
Uz ovakve promjene u zakonu se dalo do znanja kako su internet i općenito računalne mreže značajni javni mediji te da je potrebno oprezno pristupati s izjavama na istima, kao i radnjama za koje do sad nije bilo propisanih kazni…

photo by: .v1ctor.

DODATAK 3a:

Zbog statusa na Facebooku ostala i bez napojnica i bez posla

dnevno.hr /vijesti/svijet/126770-zbog-statusa-na-facebooku-ostala-i-bez-napojnica-i-bez-posla.htm



Datum: petak, 04. srpnja 2014. u 16:37

Iz Texas Roadhousea javljaju da su joj otkaz dali jer je uvrijedila mušteriju pogrdnom riječju, a na Facebooku se pokrenula rasprava o tome jesu li joj trebali dati otkaz ili ne.

Konobarica Kirsten Kelly iz američke savezne države Ohio dobila je otkaz zbog, kako kaže, statusa na Facebooku u kojemu je napisala: "Ako dođete u restoran i potrošite 50 dolara ili više, trebali biste biti u mogućnosti za to dati odgovarajuću napojnicu.", piše Huffington post.

Kelly kaže da je u ponedjeljak dobila otkaz u restoranu Texas Roadhouse jer se mušterija požalila zbog njezine objave na Facebooku u kojoj se požalila na male napojnice. Poslodavac joj je rekao da je mora otpustiti jer je došla mušterija koja se osvrnula na njezinu objavu. Mušterija je vjerojatno bila jedan od Kirsteninih Facebook prijatelja, a šefu je pokazala screenshot Kirstenine objave.
Naoko bezazlen status ju je tako stajao posla. Kirsten dodaje da je u smjene bilo više ljudi čije su je napojnice iznervirale te da je svoju objavu napisala vrlo neodređeno. Iz Texas Roadhousea javljaju da su joj otkaz dali jer je uvrijedila mušteriju pogrdnom riječju, a na Facebooku se pokrenula rasprava o tome jesu li joj trebali dati otkaz ili ne.

DODATAK 3b:

Evo zašto se nije dobro hvaliti s putovanjima na Facebooku!

dnevnik.hr/vijesti/tech/evo-zasto-se-nije-dobro-hvaliti-s-putovanjima-na-facebooku---329960.html

H.J.

Brojni korisnici Facebooka često se na ovoj društvenoj mreži hvale s putovanjima te objavljuju planove o datumu polaska kao i brojne fotografije s tih putovanja. Sigurnosni stručnjaci već dugo vremena upozoravaju kako **objavljivanje takvih informacija i nije previše pametno** jer na taj način obavještavaju sve prijatelje na Facebooku (a ako imaju otvoren profil do tih informacija može doći više od milijardu ljudi) kako u određeno vrijeme neće biti doma, što je **'pozivnica za lopove' koji točno znaju kad će kuća ili stan biti prazni.**

- 'Podigla je ljestvicu glupih objava na Facebooku na novu razinu'

Amerikanka **Stacey Grant** nije se pridržavala ovih savjeta te je sve prijatelje na Fejsu redovno obavještavala o svojim planovima za odlazak u Las Vegas, a ove je informacije iskoristio njen 'prijatelj' s Facebooka **Michael Batson** koji je, **dok je ona bila na putu, zajedno s još dvojicom provalnika opljačkao njen stan.**

Nakon što se Stacey pohvalila kako je stigla u Las Vegas, on joj je čak poslao SMS kako bi se uvjerio da je ona zaista tamo. Samo nekoliko sati nakon što mu je odgovorila na poruku, policija je kontaktirala Stacey i obavijestila je o provali u njenu kuću tako da se odmah morala vratiti s putovanja te se šokirala kada je saznala što se dogodilo. **'Bilo je bolno! Cijela soba mi je uništena, odjeća je bila posvuda'**, u suzama je rekla novinarima NBC Los Angelesa.

- Kakav šok! Evo što se događa kada ne zaštitite svoju privatnost na Facebooku

Stacey je imala puno sreće jer se čini da su provalnici uhićeni slučajno – naime, policajci su već bili u njenom susjedstvu kada su vidjeli tri mladića kako iznose stvari iz kuće i ubacuju ih u kamion.

Oni su odmah uhićeni te očekuju suđenje zbog provale i krađe, a glasnogovornica policijske postaje u Fontani u Kaliforniji **Martha Guzman-Hurtado** komentirala je novinarima kako je ovo još jedan dokaz kako bi ljudi trebali **'biti jako pažljivi oko sadržaja kojeg objavljuju na društvenim mrežama'** jer nikada ne mogu biti sigurni kada bi netko mogao iskoristiti te informacije i fotografije.

DODATAK 3c:

Upozorenje građanima

mup.hr/193342/3.asp

8. rujan 2014. objavljeno u 13:01

U proteklih nekoliko dana evidentirano je da korisnici telekomunikacijskih usluga putem SMS poruke dobivaju poruke sadržaja „Nazovi me hitno“ ili zaprimaju pozive s nepoznatih brojeva prilikom čega korisnicima ostaje obavijest o propuštenim pozivima. Pozivanje brojeva koji počinju s +224xxxxxxx, +225xxxxxx i +216xxxxxx može rezultirati neželjenim troškovima jer navedeni brojevi spadaju u ZONU 2 (Afrika) tj. pripadaju državama +224 Gvineja, +225 Bjelokosna Obala, +216 Tunis.

Upozoravamo građane, korisnike telekomunikacijskih usluga kako su se pojavili i dolazni pozivi s gore spomenutih brojeva te se pozivatelji u tim slučajevima lažno predstavljaju i korisnike traže osobne podatke i zahtijevaju da izvrše određene uplate novčanih sredstava. Osobe koje zaprime takav poziv savjetujemo da ni u kom slučaju ne daju svoje osobne podatke, niti da uplaćuju novčana sredstva nepoznatim osobama.

Nažalost, ovo nije prvi slučaj ovakve vrste prijevara te ponovo savjetujemo građanima da ne odgovaraju na ovakve i slične poruke i pozive, a ukoliko sumnjaju u vjerodostojnost pošiljatelja, odnosno ukoliko im je telefonski broj s kojeg je poruka stigla ili s kojeg je upućen poziv nepoznat, slobodno se obrate svome operateru te provjere navedeni broj.

DODATAK 3D:

'Ovo je zlostavljanje, nema veze što su djevojke same stavile slike na Facebook'

dnevnik.hr/vijesti/hrvatska/mala-se-roka-od-7-razreda-ovo-je-zlostavljanje-nema-veze-sto-su-djevojke-same-stavile-slike-na-facebook---332849.html

Zagreb, 22.04.2014., 17:16
Autor: T.V.
66 komentara

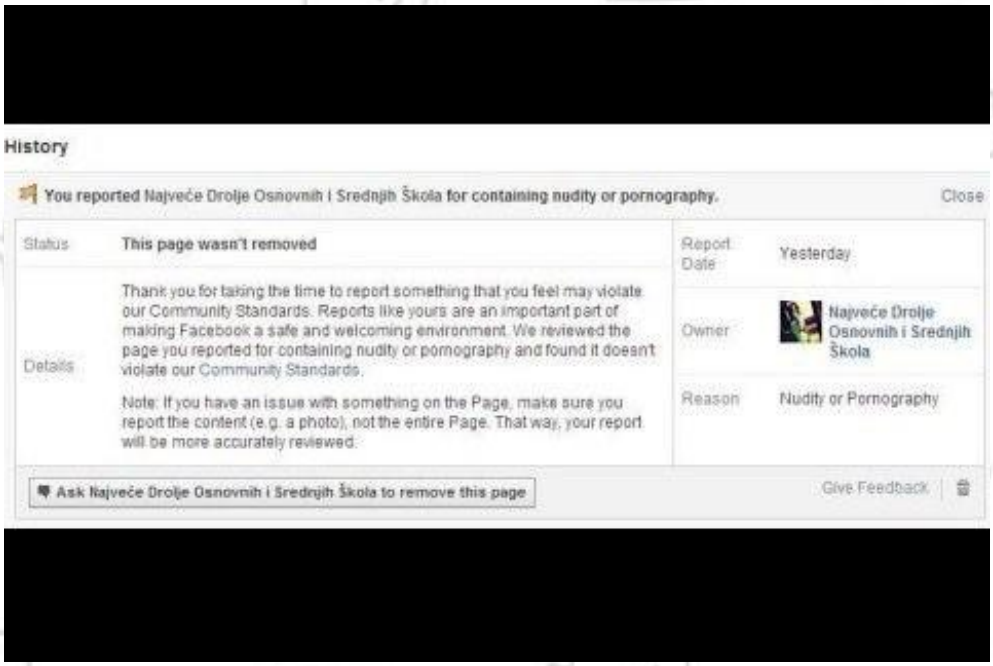
Više od 66.000 osoba 'lajkalo' je stranicu 'Najveće drolje osnovnih i srednjih škola'. Većina njih u toj stranici vjerojatno ne vidi ništa sporno

Uvredljiva stranica (Video: Dnevnik Nove TV)

Proteklih dana digla se velika prašina oko Facebook grupe 'Najveće drolje osnovnih i srednjih škola' na kojoj su objavljene na stotine fotografija, uglavnom maloljetnica iz regije koje su i one same, prethodno pojavi grupe, objavile na svojim Facebook profilima.

Pokretač grupe, navodno maloljetni Hrvat, ne vidi ništa sporno u ovoj stranici te je sve djevojke čije je slike objavio počastio komentarima poput 'Primila više kur*** nego što ima godina', 'Ova nije ni kurva ni drolja, ovo je droljetina žešća', 'Mala se roka od 7. razreda' te još brojnim sličnima.

Mnogi korisnici Facebooka prijavili su ovu grupu, no zaprimili su odgovor kako grupa nije ugašena jer 'ne krši standarde'. **Radi se o tome da je stranica prijavljivana pod kategorijom 'Pornografije i seksualno eksplicitnog sadržaja' kojeg u doslovnom smislu na stranici nem**a zbog čega ona još nije uklonjena s društvene mreže.



Istina da se djevojke danas naslikavaju od rane dobi u vrlo provokativnim pozama zbog čega se vraćamo na priču o privatnosti na društvenim mrežama i nadzoru nad profilima maloljetnika koji bi u svoje ruke trebali preuzeti roditelji ili bar educirati djecu o tome kakve se stvari ne bi smjele objavljivati.

- Žrtva pedofilske grupe: Sramim se jer sam završila u nekoj grupi pod nazivom 'drolja'

Upravo na to ukazuje i pravobraniteljica za djecu Ivana Milas Klarić koja kaže kako je **zgrožena razmjerima i brutalnošću zlostavljanja djece i mladih putem Facebooka**. Postoji mogućnost i da se putem Europske mreže pravobranitelja za djecu ENOC-a (European Network of Ombudspersons for Children) pokušaju ispitati mogućnosti bolje zaštite mladih na društvenim mrežama.

'Čini se da i naš pravosudni sustav mora pronaći učinkovitije odgovore na ovakve slučajeve, a svakako mislim da bi i davatelji usluga društvenih mreža, u ovom slučaju Facebook, trebali pokazati više društvene odgovornosti i spriječiti ovakvo zlostavljanje. Jer **ovdje je nedvojbeno riječ o cyberbullyingu, neovisno o tome što su pritom iskorištene slike djevojčica i djevojaka koje su one same objavile**', kaže pravobraniteljica Milas Klarić.

Jasno je da je ovaj konkretan slučaj nije u nadležnosti samo jedne osobe ili institucije. No, ipak je najvažnije o svemu propisno educirati djecu. **'Smatram da je najvažnija preventiva, koja mora obuhvatiti ne samo djecu, već i roditelje. Jako je važno uputiti roditelje da i sami poštuju privatnost svoje djece,** da budu oprezni kad objavljuju vlastite slike na Facebooku, a pogotovo kad objavljuju slike djece, kao i da nadziru aktivnosti mlađe djece na internetu. Ako djeca i mladi baš moraju imati svoj profil na Facebooku, neka to bude što kasnije kad već budu dovoljno zrela da se mogu zaštititi', dodaje pravobraniteljica.

I doista, dok se sustav ne promijeni i dok društvene mreže same ne stanu na kraj cyberbullyingu jedini način izbjegavanja ovakvih situacija jest objasniti djeci koliko su ranjiva na internetu, posebice na društvenim mrežama. Pogotovo kad znamo da **sve ono što se jednom na Facebooku objavi zauvijek ostaje negdje u bespuću internetskih prostranstava.**

DODATAK 4: kako zaštititi svoju privatnost na internetu[8]

1) Oni pitaju, vi ne kažete.

Samo zato što vas pitaju, ne znači da vi morate odgovoriti. Ako samo izrađujete profil za elektroničku poštu, nema potrebe za sveobuhvatnim profilom, a ako se pridružujete nekoj društvenoj mreži, možete ograničiti količinu osobnih podataka koje dajete na minimum. Kada vam nije potreban odgovor, uvijek možete jednostavno izmisliti neku adresu e-pošte.

2) Kolačići su najbolji kada se mogu pojesti.

Pazite da samo internetske stranice koje posjećujete smiju prikupljati informacije u obliku kolačića (tzv. cookies) tako što ćete podesiti svoj preglednik da odbacuje kolačiće trećih strana. Na ovaj način smanjujete mogućnost krađe podataka od strane beskrupuloznih 'trackera' , primjerice, putem lažnih oglasa ugrađenih u stranice koje posjećujete.

3) Lozinke, ne putovnice

Pobrinite se da vaše lozinke štite vaše podatke, a ne da služe kao putovnica prema vašim osobnim podacima. Ne koristite svugdje istu lozinku i ne upotrebljavajte korisničko ime s jedne stranice kao lozinku na drugoj jer hakeri mogu uspoređivati podatke. Upotrebljavajte brojke i slova, neka štampana, u kombinacijama koje nisu riječi iz rječnika.

4) Vi dajete besplatno, oni to prodaju.

Kopajte malo i pogledajte profile drugih ljudi – što možete pročitati o njima, oni mogu pročitati o vama. Objavljivanje fotografija može biti problem. Jednom kada ste svoje osobne fotografije stavili na internet imat ćete jako malo kontrole nad njihovom upotrebom. Još uvijek želite popuniti sve one detaljne podatke?

5) Svoje osobne podatke držite pod ključem

Društvene mreže su zlatni rudnik za skupljače podataka, zato im otežajte život najrigoroznijim postavkama zaštite privatnosti. U žustroj raspravi može vam se dogoditi da kažete više nego ste željeli, stoga provjerite što ste objavili kako bi bili sigurni da vam nikakvi osobni podaci nisu 'pobjegli'.

6) Zatvorite prva vrata prije nego otvorite sljedeća

Ostati prijavljen na svoj račun na društvenoj mreži ili bankovnom računu isto je što i ostaviti otključan auto: potpuno ste otvoreni upadu hakera. Izbjegnite zato rizik i odjavite se iz svojih računa prije nego nastavite pregledavati Internet.

7) Tko se prikrpao vašoj mreži?

Ako koristite bežičnu mrežu pazite da nemate uljeze, osiguravanjem svoje mreže sa što zahtjevnijom lozinkom, kriptiranom snažnijom WPA enkripcijom, gdje je to moguće.

8) Sigurnost je dvosmjerna ulica

Vi možda pazite na sigurnost računala i vaših podataka na internetu, no što je s onima koji te podatke spremaju? Izabrali ste najviše sigurnosne postavke, ali ako neka internetska stranica ne može držati vaše podatke na sigurnom onda ste još uvijek ranjivi. Koliko se pouzdani vlasnici stranice i njihovi sigurnosni sustavi?

9) Ograničavanje štete

Razmotrite korištenje metode plaćanja koja je samo za internetsku kupovinu. Postavite nizak kreditni limit tako da u slučaju krađe lopov ne može napraviti veliku štetu.

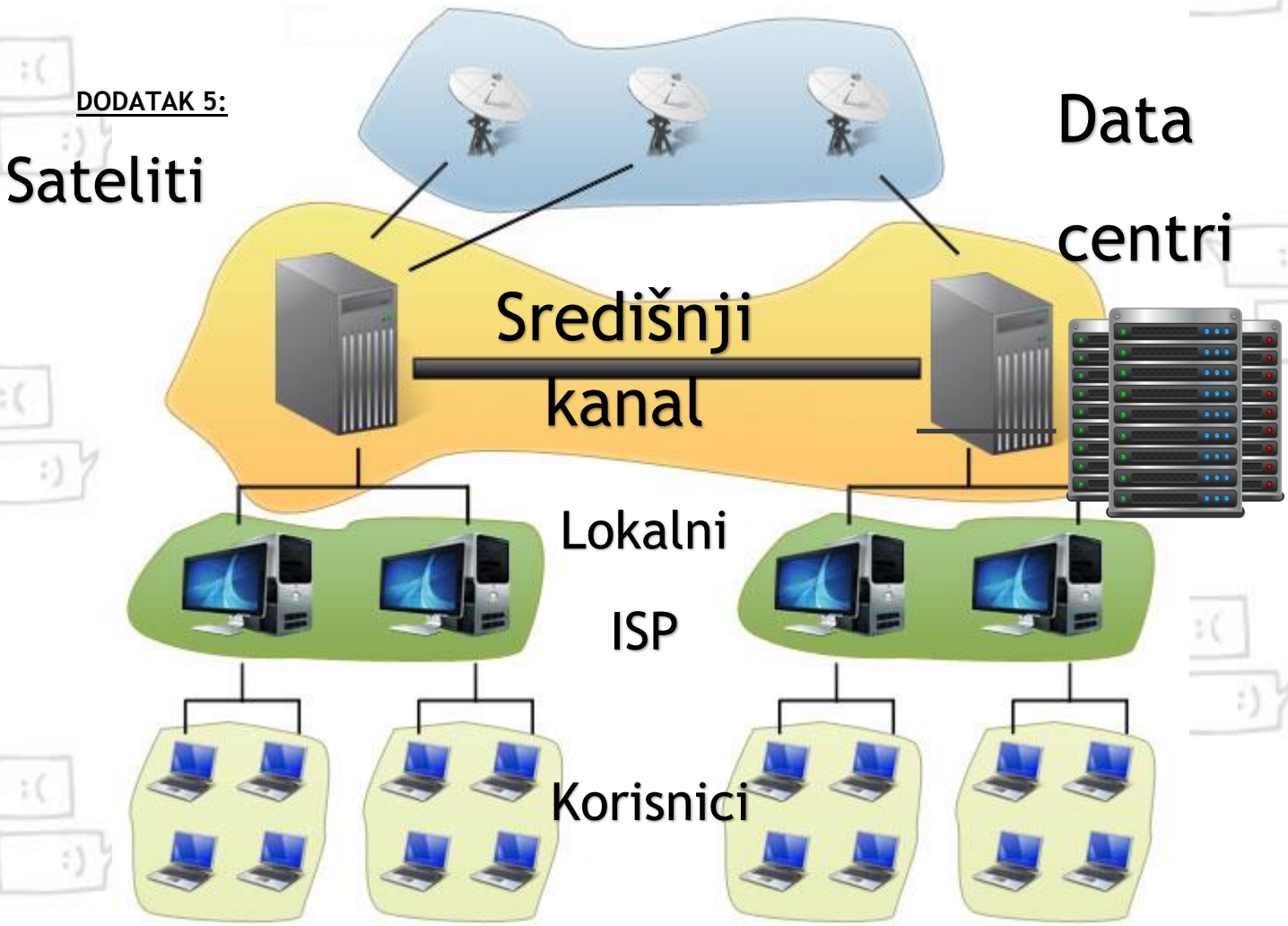
10) Što velika slova daju, mala uzimaju

Ono što vrijedi za sve, vrijedi i za Internet – pazite što potpisujete. Primjerice, neki ugovori automatski se obnavljaju i morate se u određenom trenutku izjasniti protiv produženja ako ne želite da vam se kreditna kartice tereti.

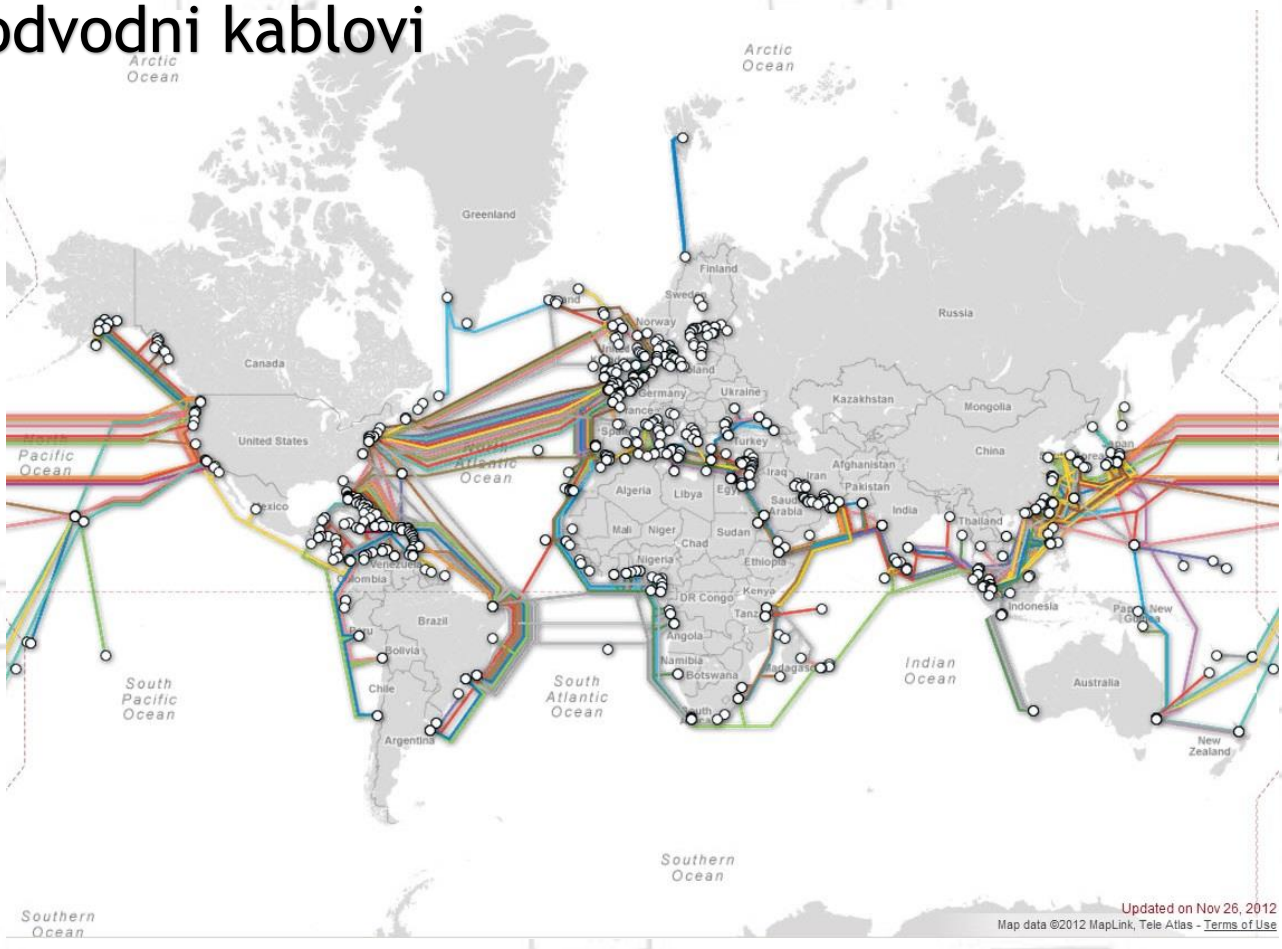
[8] http://www.europarl.europa.eu/news/hr/news-room/content/20131003STO21413/html/10-savjeta-Kako-za%C5%A1tititi-privatnost-na-internetu

Internet

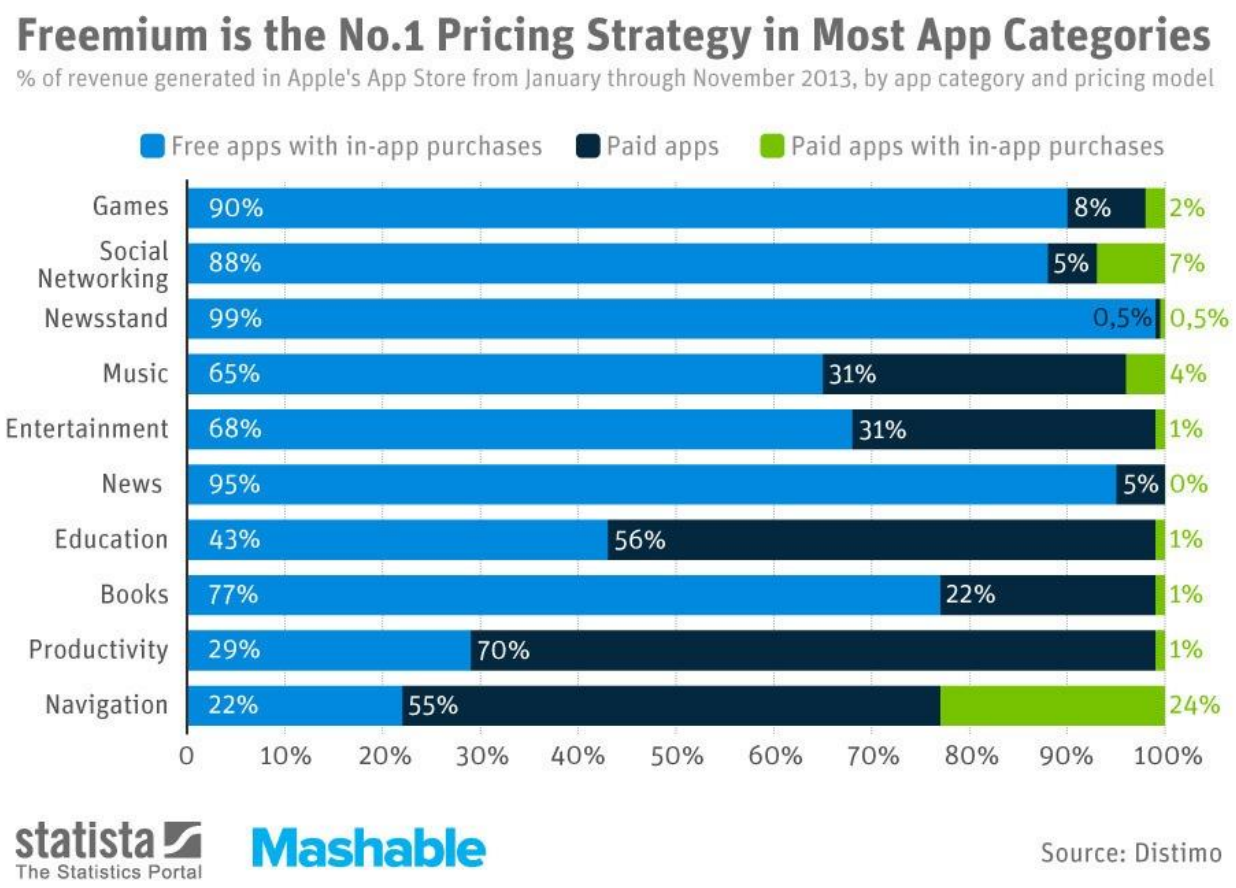
DODATAK 5:

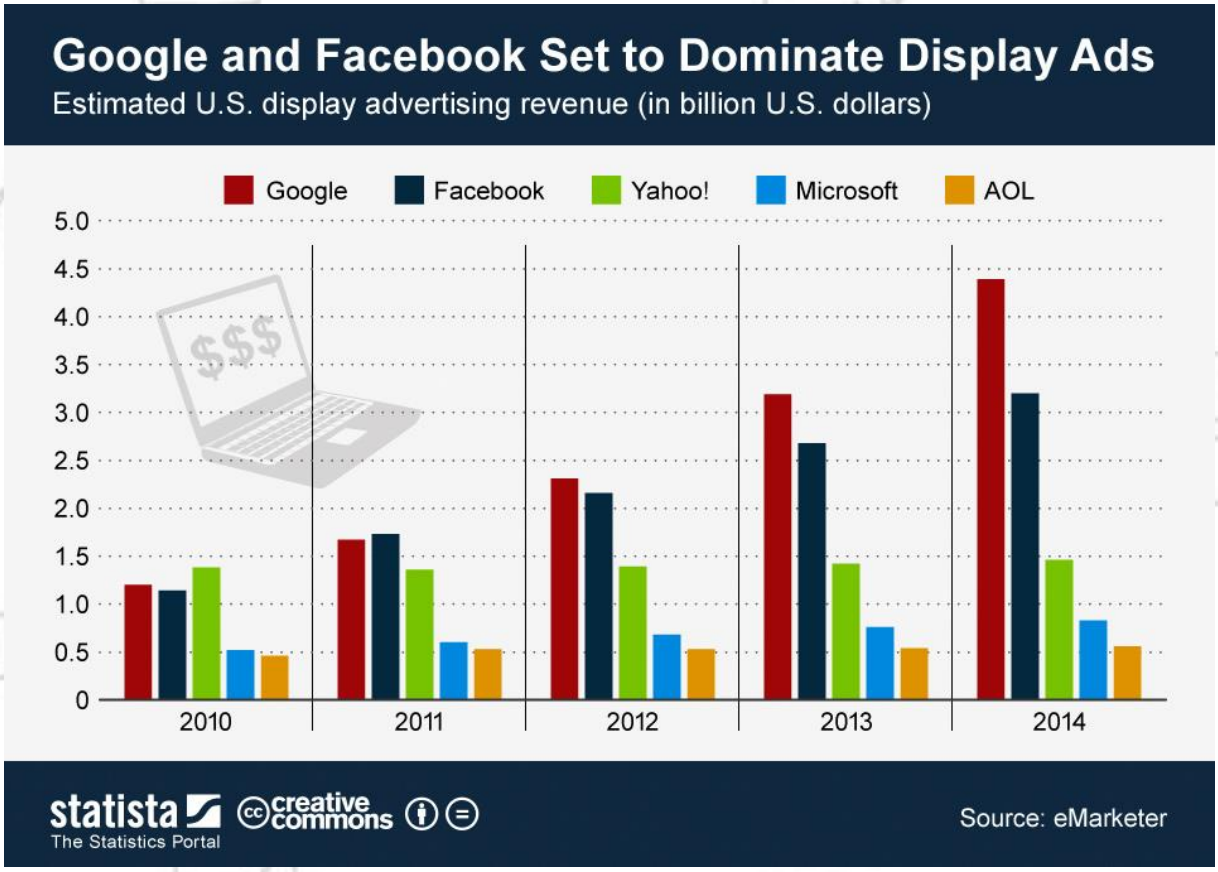


Podvodni kablovi



DODATAK 6:

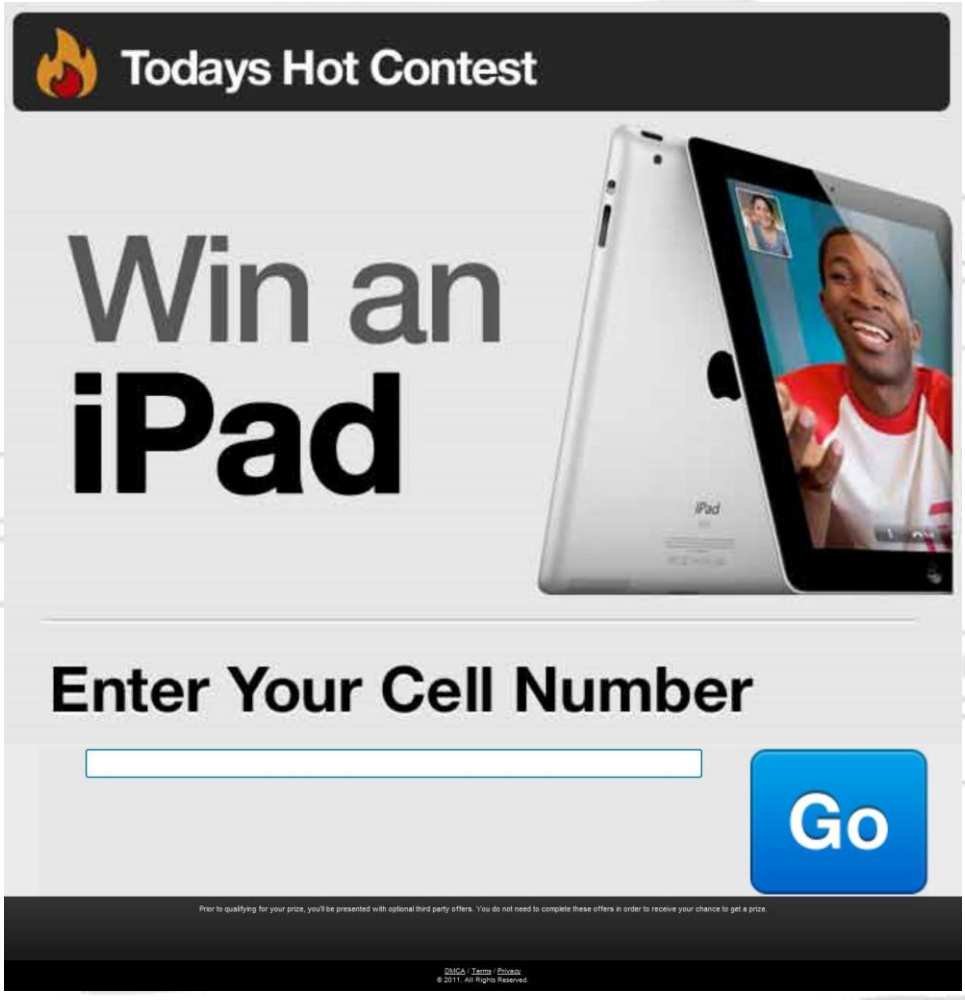

Freemium is the No.1 Pricing Strategy in Most App Categories
% of revenue generated in Apple's App Store from January through November 2013, by app category and pricing model
Free apps with in-app purchases
Paid apps
Paid apps with in-app purchases
Games 90% 8% 2%
Social Networking 88% 5% 7%
Newsstand 99% 0,5% 0,5%
Music 65% 31% 4%
Entertainment 68% 31% 1%
News 95% 5% 0%
Education 43% 56% 1%
Books 77% 22% 1%
Productivity 29% 70% 1%
Navigation 22% 55% 24%
0 10% 20% 30% 40% 50% 60% 70% 80% 90% 100%
statista The Statistics Portal
Mashable
Source: Distimo


Google and Facebook Set to Dominate Display Ads
Estimated U.S. display advertising revenue (in billion U.S. dollars)
Google
Facebook
Yahoo!
Microsoft
AOL
5.0
4.5
4.0
3.5
3.0
2.5
2.0
1.5
1.0
0.5
0
$$$
2010
2011
2012
2013
2014
statista The Statistics Portal
creative commons
Source: eMarketer

DODATAK 7:


Chris
Sarah
Laura
Dan
James


[redacted]
June 23, 2013
Me
You
Like · Comment · Share
4


Todays Hot Contest
Win an
iPad
Enter Your Cell Number
Go
Prior to qualifying for your prize, you'll be presented with optional third party offers. You do not need to complete these offers in order to receive your chance to get a prize.
DMCA | Terms | Privacy
© 2011. All Rights Reserved.

Zahvale i izvori

http://screwsandmarbles.wordpress.com/2013/06/14/tor-is-not-magic/

http://www.softicons.com/web-icons/web-hosting-icons-by-heart-internet/data-center-icon

http://www.sweetmaps.com/blog/wp-content/uploads/2012/11/submarinecablemap.jpg

http://www.boostingecommerce.com/e-commerce-trends-and-statistics-in-europe

http://www.international-television.org/tv_market_data/online-advertising-world-usa-europe_2005-2012.html

http://mashable.com/2013/12/19/paid-vs-free-apps/

http://www.statista.com/chart/620/estimated-display-advertising-revenue-of-major-digital-ad-selling-companies-in-the-united-states/

http://www.tnooz.com/article/google-versus-facebook-from-an-advertising-perspective-infographic/

http://yourstory.com/2014/03/ultimate-master-list-revenue-models-web-mobile-companies/

http://latticelabs.com/blog/2013/09/premium-freemium-subscription/

http://jimshowalter.blogspot.be/2012/02/comparison-of-various-software-revenue.html

http://www.fastcompany.com/1768119/do-social-networks-really-compete-google-vs-linkedin-round-one

http://www.forbes.com/sites/erikkain/2013/05/09/as-world-of-warcraft-bleeds-subscribers-free-to-play-is-already-winning-the-future/

http://www.gamasutra.com/blogs/SheldonLaframboise/20130806/197655/Why_Freemium_Feels_So_Damn_Good_in_League_of_Legends.php

http://blogs.wsj.com/cmo/2014/07/15/cokes-personalized-marketing-campaign-gains-online-buzz/

DODATNE INFORMACIJE:

The #DeleteCyberbullying projekt financira DAPHNE III program EK kojim koordinira COFACE[9].

Prema definiciji Europske komisije, Cyberbullying je opetovano verbalno ili psihološko uznemiravanje koje provodi pojedinac ili skupina protiv drugih. Ima mnogo oblika: ruganje, uvrede, prijetnje, glasine, tračanje, "happy slapping", neprilični komentari ili kleveta. Interaktivni internetski servisi (e-pošta, sobe za chat, instant dopisivanje) i mobilni telefoni nasilnicima su pružili nove mogućnosti i načine zlostavljanja svojih žrtava.

Nekoliko ciljeva projekta #DeleteCyberbullying:

Općenito priznanje da je cyberbullying stvarna i znatna opasnost te uzrokuje neposrednu i značajnu štetu.

Razmjena najboljih praksi vezanih uz prepoznavanje, nadzor i prevenciju štetne on-line komunikacije i cyberbullyinga, naročito u školi i obitelji.

Posebne preporuke donositeljima odluka o politici na razini EU i zemalja članica - primjeri preventivnih kampanja s pozitivnim učinkom.

Razvoj on-line kampanje i materijala te **poticanje uključivanja djece** i mladih, za koje ne želimo da budu više od krajnjih korisnika projekta, već i da preuzmu vlasništvo u ovom problemu i postanu dio društvenih i promjena ponašanja koje bismo željeli postići.

Za više informacija o projektu, posjetite našu stranicu www.deletecyberbullying.eu ili pošaljite e-poštu na secretariat@coface-eu.org

ODRICANJE OD ODGOVORNOSTI:

Ovaj priručnik proizveden je uz financijsku potporu DAPHNE III Programa[10] Europske Unije. Sadržaj ovog priručnika je isključiva odgovornost COFACE-a i ne može se smatrati da odražava gledišta Europske komisije.

[9] www.coface-eu.org
[10] http://ec.europa.eu/justice/grants/programmes/daphne/index_en.htm

Licenca:

creative commons

COMMONS DEED

Dozvoljeno je:

- kopiranje, distribucija, prikazivanje i provedba nastavnih aktivnosti

Pod sljedećim uvjetima:

Autorska prava. Poštujte pravila navođenja izvora koje propisuje autor ili dobavljač.

Zabranjena prodaja. Zabranjeno je koristiti ovaj priručnik u komercijalne svrhe.

Zabranjeno nadograđivati. Nije dozvoljeno mijenjati, preoblikovati ili nadograđivati ovaj priručnik.

Slobodni ste koristiti priručnik po gore navedenim načelima.

Udruga roditelja „Korak po korak“ suradnik je na projektu #DeleteCyberbullying, koji provodi Konfederacija obiteljskih organizacija Europske unije (COFACE) uz financijsku podršku programa EU DAPHNE u 14 europskih zemalja.

Udruga roditelja „Korak po korak“ prevela je i prilagodila materijale (priručnik, aplikaciju i video) na hrvatski jezik.

Za sve informacije o provedbi projekta u Hrvatskoj možete se obratiti Udruzi roditelja „Korak po korak“.

Udruga roditelja
KORAK PO KORAK

Udruga roditelja "Korak po korak"
Ilica 73, 10000 Zagreb

Tel.: 01 48 55 578
fax: 01 4847 598

E-mail: info@udrugaroditeljakpk.hr
www:udrugaroditeljakpk.hr