

Vodič za siguran internet i nepromišljene surfere

Kako se zaštititi u svijetu interneta i mobilnih uređaja?



HRVATSKA REGULATORNA AGENCIJA
ZA MREŽNE DJELATNOSTI



1. Dragi učenici (surferi), nastavnici, roditelji!

Znamo da već uživate u mnogim pozitivnim aspektima online svijeta, no želimo vas još jednom upozoriti kako uz sve dobrobiti koje nam internet pruža dolaze i određeni rizici.

Sjećate li se svojih prvih, dječjih istraživanja interneta? Niste odmah postali znalci; trebalo vam je vremena i truda da otkrijete sve mogućnosti koje poznajete danas. Na isti način, strpljivo i mudro, trebate stjecati i znanje o tomu kako se zaštititi i ostati sigurni dok istražujete digitalni svijet. Tehnologija se jako brzo razvija i taj razvoj traži od nas da budemo još bolje informirani i spremniji prepoznati dobre i loše strane koje nam internet nudi.

Vjerujemo da su vam osnove sigurnosti na internetu već poznate, a uz malo dodatne odgovornosti, znanja i otvorenosti u komunikaciji s roditeljima i nastavnicima, možete uživati u svim prednostima koje vam otvoreni virtualni svijet nudi i to bez straha od opasnosti koje se mogu pojaviti.



2. Tko smo mi?

Uz brojne i važne poslove koje obavljamo, u HAKOM-u imamo i posebnu zadaću – promicati i poticati zaštitu djece na internetu.

Svake godine, drugog utorka u veljači, priključujemo se globalnoj inicijativi organizirajući posebne aktivnosti usmjerene promicanju sigurnog korištenja interneta, čime obilježavamo Dan sigurnijeg interneta. To je manifestacija koja se smatra najznačajnijim događajem u kalendaru informacijske sigurnosti i provodi se istovremeno u preko 140 država svijeta s istim ciljem – promicanja sigurnijeg i odgovornijeg korištenja tehnologije. Za učenike svih osnovnih škola u RH pripremamo brošure s korisnim savjetima o tome kako sigurno koristiti internet i trudimo se da vas one dočekaju u školskim klupama. Ta brošura, koju držite u rukama, ima za cilj pomoći djeci i roditeljima da bolje razumiju kako se zaštititi dok *surfaju* internetom.

No, to nije sve! Već duži niz godina provodimo i poseban projekt zaštite djece na internetu i u svijetu mrežnih tehnologija. Naši stručnjaci rado posjećuju zainteresirane osnovne škole i održavaju radionice s djecom i roditeljima, kako bi ih posavjetovali o odgovornijem ponašanju na internetu.



Na taj način zajedno učimo kako se zaštititi i kako koristiti internet odgovorno, a kako bismo mogli bezbrižno uživati u *online* svijetu!

Prvo što želimo istaknuti je važnost roditeljske podrške i komunikacije. Svejedno je koliko godina imate; roditelji su tu da vas podrže i odgovore na vaša pitanja. Nikad se ne ustručavajte zatražiti od njih pomoć ako imate bilo kakvih problema ili nejasnoća.

S obzirom da je gledanje videa postao jedan od načina za učenje i zabavu, za vas smo izradili i poseban video o sigurnosti na internetu. Možete ga pogledati na našem YouTube kanalu. Glavna poruka videa je da uvijek možete razgovarati s bliskim odraslim osobama o svojim *online* iskustvima i problemima. Zato je za pozitivan odnos djece i roditelja važno povjerenje.

Ako imate bilo kakvih prijedloga ili komentara o tome kako bismo mogli bolje podržati vas i vaše potrebe na internetu, slobodno nas kontaktirajte na zastita-djece@hakom.hr. Vaše mišljenje jako nam je važno!

Zapamtite, internet je odličan izvor informacija, ali važno je znati kako se zaštititi i koristiti ga odgovorno. HAKOM je tu da vam pomogne na tom putu, stoga nam šaljite prijedloge o tome što želite naučiti u novim brošurama koje radimo za vas.



**Zaštita
djece na
internetu**



**Luka
Bulić –
sigurniji
internet**

3. Internet danas

U stvarnom svijetu postoje granice ponašanja i državne granice koje određuju gdje možete ići i što možete raditi. Međutim, na internetu te granice ne postoje, barem ne u vidljivom obliku, a to znači da možete komunicirati s osobama diljem svijeta, pristupati informacijama iz bilo kojeg kutka svijeta i sudjelovati u razgovorima u globalnim zajednicama.

To je zaseban svijet u kojem se informacije i ljudi kreću slobodno, no sloboda također zahtjeva i odgovornost. Na internetu morate biti pažljivi i odgovorni jer se pravila i zakoni mogu razlikovati od zemlje do zemlje. Također, morate se brinuti o svojoj *online* sigurnosti i poštovati druge korisnike.

U tom digitalnom svijetu često se izlažemo dobrom sadržaju, učenju, zabavi, ali i nekim lošim stvarima poput prevara i kriminalnih aktivnosti. Bez obzira na to iz koje zemlje dolazimo i kojim jezikom govorimo, važno je uvijek biti svjestan tih činjenica.

Mi ljudi smo beskrajni optimisti i često živimo u uvjerenju da nam se ništa loše neće dogoditi na internetu, da se neugodne situacije događaju drugima i ono najgore - da nismo dovoljno važni ni zanimljivi da bi upravo nas netko pokušao prevariti! Na žalost, ništa od toga nije istina!

Osnovna pravila koja moraš poznavati prilikom korištenja interneta su:

- 1. Čuvaj svoje osobne podatke:** Ne dijeli svoje pravo ime (koristi *nickname*), adresu (isključi lokaciju), broj telefona i druge osobne podatke s nepoznatim osobama na internetu.
- 2. Pazi na lažne informacije:** Na internetu se može pronaći puno lažnih informacija. Uvijek provjeri jesu li informacije pouzdane prije nego u njihovu točnost povjeruješ.
- 3. Budi oprezan s porukama:** Ne otvaraj poruke od nepoznatih osoba i ne odgovaraj na njih. Ponekad ljudi nemaju dobre namjere i šalju neprimjeren sadržaj.
- 4. Pomozi roditeljima:** Ako naiđeš na nešto čudno ili te nešto brine, reci to bez straha svojim roditeljima. Oni su tvoji saveznici od prvog dana. Ne strahuj da će se ljutiti – prije će biti razočarani što nisu bili prve osobe kojima si se obratio za pomoć.



4. Odgovornost čuvanja podataka o sebi

Jeste li se ikad, dok koristite Internet, zapitali koliko su važni vaši osobni podaci?

Zaštita osobnih podataka je zapravo jako važna u *online* svijetu, zar ne?

Pristupni podaci su tvoji digitalni ključevi, koje koristiš kako bi se prijavio na različite *online* usluge.

Identificiranje znači potvrdu kojom potvrđuješ “Ja sam taj!” u trenutku kad koristiš te ključeve.

Autentificiranje je način na koji sustav provjerava jesi li stvarno osoba kojom se predstavljaš.

Ako pristupni podaci nisu dovoljno jaki i sigurni netko drugi ih može ukrasti i preuzeti tvoj identitet. To znači da bi lako mogli koristiti tvoje lozinke i predstavljati se kao ti, što je zbilja loše i može biti opasno! To je kao da netko neovlašteno ulazi u tvoj dom i radi što hoće.

Zaštiti svoje pristupne podatke - koristi jake lozinke i redovito ih mijenjaj. Nemoj ih dijeliti ni s kim (čak ni s najboljim prijateljem) - to su tvoji tajni ključevi u *online* svijetu!

Biometrija je još ozbiljnija stvar - to su posebni načini autentificiranja koji koriste tvoje jedinstvene tjelesne karakteristike poput otiska prsta, lica ili zjenica oka. Na primjer, kad otključavaš telefon koristeći otisak prsta ili putem prepoznavanje lica - to je biometrija. Ona je dodatna razina sigurnosti koju koristiš kako bi zaštitio svoj uređaj.



Kakve lozinke koristiti

Dobra lozinka morala bi biti dovoljno kompleksna i dugačka da ju je teško ili nemoguće lako probiti čak i jačom računalnom snagom, a opet dovoljno pamtljiva da je ne zapisuješ po papirićima.

Svoje ćete lozinke učiniti sigurnima ako:

- *Koristite lozinke s više od deset (10) znakova za korisničke račune te petnaest (15) za privilegirane račune*
- *Ne ponavljate lozinke*
- *Koristite velika i mala slova, brojeve, kao i neke od specijalnih znakova (-, !, ?, &, #, %, *, 4).*
- *Koristite fraze koje samo vama nešto znače - npr. ako ste davno jeli odlično jelo, lozinka bi mogla biti (bez navodnih znakova) „odlicanLavacake75naBracu“- vama je lako pamtljiv događaj za koji drugi ne znaju, pri tomu koristite mala i velika slova, brojeve te specijalne znakove, a sve skupa ima 25 znaka, što je s današnjom tehnologijom praktički neslomljivo.*

Kalkulator privatnosti

Aplikaciju Kalkulator privatnosti osmislio je HAKOM sa svojim suradnicima kako bi vam pomogli da još bolje razumijete na koji način zaštititi svoju privatnost.

Ta aplikacija je vaš *specijalni agent* za osobne podatke. Unesete li određene informacije, kalkulator će vam reći koliko su ti podaci sigurni dok *surfate* internetom, a ako primijetite da postoje rizici pomaže vam naučiti na koji način bolje zaštititi svoje tajne podatke.

Ovo je uistinu važno jer želimo da koristite internet pametno i odgovorno.

U sklopu Kalkulatora privatnosti nalazi se i Kviz o sigurnosti na internetu pa se odvažite odgovoriti na pitanja iz kviza i procijenite koliko ste spremni prepoznati moguće prevare na internetu!



Kolačići

Koliko puta ste zaprimili poruku na mobitelu: Prihvaćate li kolačiće? Jeste li ikad razmislili o tomu čemu li oni služe? Kolačići su mali digitalni tragovi koje internetske stranice ostavljaju na tvom uređaju kada ih posjetiš. To su male bilješke koje internetska stranica koristi kako bi zapamtila neke stvari o tebi i tvojim aktivnostima na internetu. Zašto su ovi kolačići bitni kad je riječ o čuvanju tvojih osobnih podataka na internetu?

1. Omogućuju internetskim stranicama da znaju što voliš pa ćeš tako vidjeti sadržaj koji te stvarno zanima, a oglasi će biti prilagođeni tvojim interesima.
2. Zbog kolačića ne moraš svaki put iznova unositi svoje podatke kad se prijavljuješ na neku internetsku stranicu.
3. Stranice koriste kolačiće kako bi pratile i analizirale tvoje interese na internetu.
4. Kolačići također pomažu u ograničavanju pristupa određenom sadržaju koji nije prikladan za tvoj uzrast, čime si zaštićen od izlaganja neprijemnim sadržajima.



5. Usluga roditeljske zaštite, ljeti li vas to?

Mnogi roditelji koriste alate ili uslugu roditeljske zaštite kako bi vas zaštitili od potencijalnih rizika na internetu. Usluga roditeljske zaštite uključuje nadzor nad tvojom privatnosti i štiti te od neželjenih ili neprimjerenih sadržaja, ali i od osoba koje na mreži nemaju dobre namjere.

Ako smatraš da je tvoja privatnost povrijeđena te da je nadzor suvišan, pokaži sam koliko možeš biti umjeren i odgovoran i stoga svakodnevno u postavkama, pod digitalnom dobrobiti/roditeljska zaštita, provjeri koliko vremena i na kojim aplikacijama provodiš dio dana/tjedna.

Ako smatraš da je roditeljska zaštita „dosadna“, instaliraj aplikaciju **Forest app** koja ti omogućava da sam odrediš koliko vremena ne želiš koristiti mobitel, a za vrijeme tvog online odsustva u aplikaciji rasti će drvo. Ako povratak iz offline svijeta bude prebrz, drvo neće narasti nego će propadati.

Provjeri rasteš li ili veneš!



**Forest
App**



Savjet za roditelje!



Operatorima je propisana obveza, ako postoji tehnička mogućnost, ponuditi svim korisnicima opciju postavljanja zabrane pristupa sadržaju koji nije namijenjen djeci. Prigodom prvog potpisivanja ugovora, operatori ili njegovi ovlašteni prodavači, obvezni su ponuditi takvu mogućnost. Ako korisnik odabere navedenu opciju, može je početi koristiti bilo kada za vrijeme trajanja ugovora te će ona biti omogućena sve dok korisnik ne zatraži ukidanje.



Ako djeca prime SMS ili MMS poruke sa sadržajem koji im nije primjeren i namijenjen je isključivo odraslima, o tome možete obavijestiti svog operatora ili prijaviti primitak takve poruke na adresu elektroničke pošte nezeleni.sms@hakom.hr. Brojevi s kojih se šalju takve poruke će se nakon provjere u najkraćem mogućem roku blokirati.

Zabrana slanja i/ili primanja SMS i MMS poruka u okviru usluge s posebnom tarifom (6xx xxx, 8xx xxx i sl.) može se besplatno zatražiti od operatora.

Moguće je postaviti zabranu korištenja usluga nakon dogovorenog limita potrošnje u iznosu od 7,00 €.

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

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

6. Pismenost

Pismenost podrazumijeva sposobnost čitanja i pisanja, razumijevanja i komunikaciju putem pisanih i govornih riječi. To znači da možeš čitati knjige, razumjeti što piše u njima, napisati poruke ili eseje te komunicirati s drugima usmeno kako bi podijelio informacije ili razgovarao s prijateljima.

Više je različitih vrsta pismenosti, a u svijetu digitalnih tehnologija posebno su bitne digitalna pismenost (poznavanje mogućnosti računala i interneta) i medijska pismenost (shvaćanje kako mediji oblikuju informacije). Svaka vrsta pismenosti, pa i one koje nismo posebno istaknuli, uči te vještinama i sposobnostima koje ti pomažu snaći se u svakodnevnom životu, učenju i komunikaciji s drugima. Pismenost je osnovna vještina koja omogućava ne samo pristup informacijama, već i njihovo razumijevanje, procjenu pouzdanosti, učenje, a time i aktivnu uključenost u društvenu zajednicu.



Razlike između medijske, informacijske i digitalne pismenosti!



1. Medijska pismenost: to je sposobnost razumijevanja informacija koje vidite, čitate i slušate u medijima. Pomaže vam shvatiti kako mediji oblikuju informacije i poruke.

Primjer: Prepoznavanje lažnih vijesti na društvenim mrežama

Kada vidiš sadržaj koji ti privlači pažnju (npr. koliko zarađuje vaš *youtuber?*), važno je zapitati se tko je autor vijesti, koliko je medijski izvor vjerodostojan, jesu li informacije realne i na koji način mogu provjeriti je li ono što je navedeno istinito. Bitno je razlikovati pouzdane izvore od onih koji to nisu te provjeriti i kritički promisliti je li vijest koju si čuo ili pročitao istinita ili ne, prije nego što informacije podijeliš s prijateljima.



2. Informacijska pismenost: odnosi se na sposobnost pronalaženja, provjeravanja i korisne upotrebe informacija. Važno je naučiti kako razlikovati korisne informacije od suvišnih i na koji način koristiti informacije za rješavanje problema.

Primjer: Istraživanje školskih projekata

Tijekom rada na školskom projektu informacijska pismenost pomaže nam u efikasnijem traženju i korištenju informacija, pravilnom citiranju izvora i u konačnici stvaranju novih znanja.

Ta vještina istraživanja bit će ti korisna tijekom cijeloga života!



3. Digitalna pismenost: to je sposobnost korištenja računala, pametnih telefona i interneta, a razvijanjem ove vještine sigurno ćemo se kretati *online* svijetom, komunicirati s drugima i razumjeti kako ostati sigurni na internetu.

*Primjer: Koristite pametni telefon ili računalo za komunikaciju s prijateljima putem društvenih medija i razmjenu poruka. Digitalna pismenost podrazumijeva da razumijete važnost postavljanja snažnih lozinki, zaštite osobnih podataka i pravilnog postupanja u slučaju primitka sumnjivih poruka ili prijjetnji. Onaj tko zna kako održavati svoje *online* račune sigurnima, razumije osnove *online* sigurnosti i pokazuje digitalnu pismenost.*



Ove tri sposobnosti su važne jer će vam pomoći da budete pametniji i sigurniji dok surfate internetom.

7. Šifra Solidarnost: *Surferi* protiv *Online* zlostavljača



Elektroničko nasilje ili *cyberbullying* predstavlja oblik zlostavljanja koji se odvija putem digitalnih tehnologija i interneta. Evo nekoliko oblika elektroničkog nasilja s kojima se možete susresti:

1. Vrijeđanje putem društvenih mreža: uključuje slanje uvredljivih poruka ili komentara putem društvenih mreža, često sa ciljem da se osoba ponizi ili povrijedi
2. Neprestano slanje prijetećih poruka: osoba može primiti prijeteće poruke putem SMS-a, e-pošte ili društvenih mreža i one je čine nesigurnom ili uplašenom
3. Širenje lažnih glasina: netko može širiti lažne informacije o drugima putem interneta s ciljem diskreditiranja osoba ili nanošenja štete njihovom ugledu
4. Osveta putem objavljivanja slika i videa: netko može objaviti osjetljive slike ili videozapise drugih bez njihova pristanka kako bi ih sramotili
5. Stvaranje lažnih profila: stvaranje lažnih *online* profila kako bi se sprijateljili s osobom i prikupljali informacije ili širili lažne glasine
6. Izostavljanje iz *online* grupa i prijateljstava: namjerno izostavljanje osobe iz *online* društvenih grupa ili gašenje *online* prijateljstava kako bi ih izolirali

Važno je razumjeti ozbiljnost i štetu koju elektroničko nasilje može prouzročiti i znati kako se zaštititi te kako reagirati ako i sami postanete žrtva ili svjedok takvih situacija.

Što ti kao prijatelj možeš napraviti?

Ako ti je prijatelj žrtva elektroničkog nasilja:

1. Saslušaj ga i pruži mu potporu
2. Potakni ga na razgovor s odraslima čak i ako ti se čini da to nije potrebno



3. Potakni ga da prijavi zlostavljanje



ZAPAMTITE: sve što vam se događa, dogodilo se i nekom drugom prije vas!

Ako je prijatelj zlostavljač na internetu:

1. Razgovaraj s njim i potakni ga na prestanak zlostavljanja
2. Ukaži mu na ozbiljnost posljedica zlostavljanja
3. Reci mu da ne podržavaš takvo ponašanje



Kratki savjet roditeljima i nastavnicima!

Ako dijete doživi zlostavljanje putem interneta, ključno je brzo djelovati! Evo nekoliko savjeta:

1. Razgovarajte s djetetom kako bi saznali što se događa!
2. Potaknite dijete da prestane komunicirati s napadačem!
3. Sačuvajte dokaze o zlostavljanju!
4. Prijavite slučaj nadležnim tijelima i/ili pružateljima usluga!
5. Nastavite pratiti situaciju i pružite emocionalnu podršku!
6. Razmislite o sigurnosnim mjerama zaštite uređaja!
7. Ako je potrebno, potražite stručnu pomoć!

Važno je da dijete ne osjeća krivnju, a podrška odraslih njima je od ključnog značaja!

Ako primijetite da je vaše dijete zlostavljač na internetu ključno je brzo djelovati! Evo nekoliko savjeta:

1. Razgovarajte otvoreno!
2. Postavite jasne granice i pravila ponašanja!
3. Potaknite ga da prestane sa zlostavljanjem i ispriča se žrtvi!
4. Pratite njegove *online* aktivnosti!
5. Objasnite ozbiljnost zlostavljanja i posljedice koje može izazvati!
6. Ako je potrebno, potražite stručnu pomoć!

Cilj je naučiti dijete da bude odgovorno za svoje postupke i pravilno se ponaša na internetu!

8. Društvene mreže i mediji

Društvene mreže danas su nalik osobnom dnevniku u koji upisujemo sve trenutke, iskustva i događaje koje dijelimo s prijateljima. One su odličan način za održavanje veza s prijateljima i obitelji, posebno ako smo udaljeni. Omogućavaju nam komunikaciju putem poruka, komentiranje objava i daju nam uvid što ih novo zanima.

Društvene mreže su tvoj digitalni svijet u kojemu se možeš izražavati, povezivati se s ljudima i zabavljati se, ali uvijek budi oprezan kako bi ostao siguran. Kako u stvarnom životu biramo prijatelje i društvo, tako i na mreži moramo znati da nije pametno otkrivati previše osobnih informacija.



TikTok je aplikacija koju svi najradije pratite, koristite je za snimanje kratkih videa, plešete, pjevate, smijete se i zabavljate slijedeći najnovije svjetske trendove.

Kao što sami znate, neki izazovi na TikToku izazvali su ozbiljne rizike za zdravlje i sigurnost velikog broja djece i mladih u svijetu. Neki od tih izazova uključivali su fizičke radnje koje su dovele do ozbiljnih povreda kod ljudi. Zbog popularnosti na društvenim mrežama nikad se ne bi se smjeli dovoditi u takve, opasne situacije. Također, važno je da tvoj račun nije javan, a ako je i privatan ne prihvaćaj svaki zahtjev za prijateljstvom jer tako i ti postaješ javan!

Edukacija o sigurnom korištenju društvenih mreža i online sadržaja je ključna, a otvorena komunikacija s pouzdanim osobama također može pomoći u sprječavanju neodgovornih i opasnih postupaka. Zdravlje i sigurnost uvijek trebaju biti na prvom mjestu.



Snapchat je također jedna od omiljenih aplikacija zbog svojih filtera koji omogućavaju zabavu s vašim prijateljima. Unatoč tome što se poruke, fotografije i videozapisi samouništavaju nakon pregleda i što je komunikacija brza, potrebno je znati da i na ovoj mreži možete upasti u zamku ako zbog *vatra* prihvatite prijateljstvo osobe koja je zlonamjerna.

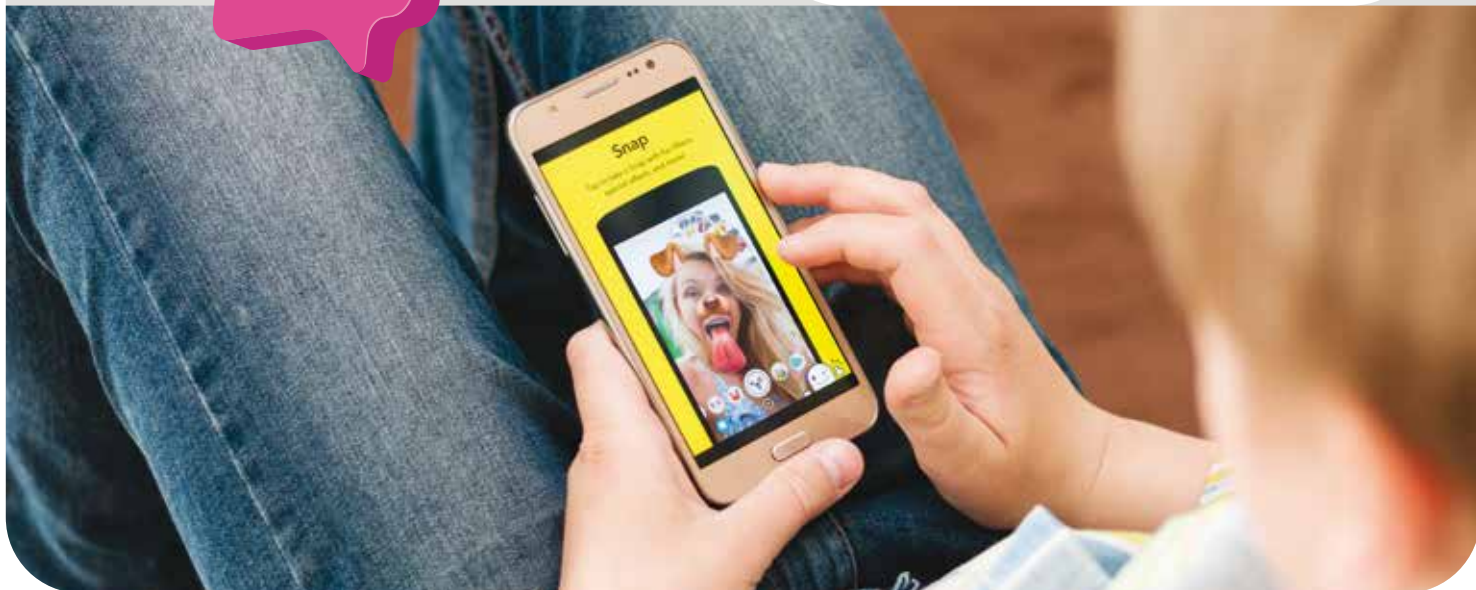


Nikad ne prihvaćaj nepoznate osobe za prijatelje!

Jako je važno blokirati ljude koji šalju neprikladne ili nasilne sadržaje, čak i ako ih poznajete!

Obavezno pripazite jeste li na Snapchatu isključili lokaciju. S obzirom na to da svi griješimo, nikad nije kasno zatražiti pomoć roditelja ili nastavnika/ce ukoliko se dogodi nešto loše!

Vaša sigurnost i dobrobit su najvažniji!



YouTube je najstarija platforma na kojoj pronalazimo video-zapise o raznim temama koje nas zanimaju. Sa sigurnošću možemo reći da je to najbolje mjesto za učenje i stjecanje novih vještina. Zaista, ne postoji više opravdanje kako nešto ne znate ili ne možete napraviti jer YouTube sadrži upute za sve.

Rizici poput neprimjerenih sadržaja i komentara prisutni su svugdje pa tako i na YouTube-u, no uvijek je važno biti svjestan potrebe *online* sigurnosti.

Među mlađom populacijom youtuberi često imaju sve veći utjecaj, a uvijek ima onih koji više vjeruju virtualnim uzorima nego obitelji i prijateljima.

Kvalitetni i popularni youtuberi mogu inspirativno utjecati na pratitelje, ovisno o sadržajima koje stvaraju i objavljuju.

Instagram je jedna od najkreativnijih platformi na kojoj je omogućeno izražavanje fotografijama i atraktivnim *storyjima*. Brojne su osobe postale poznate zbog svoje kreativnosti i napravile pravi posao, odnosno dobro su zaradile surađujući s raznim sponzorima. S obzirom na to da Instagram također služi za povezivanje s drugim korisnicima i ovdje postoje rizici kao što su neprimjereni profili, ugrožena privatnost i *online* sigurnost.

SAVJET: YouTube - moguće je regulirati sigurnosne postavke uključivanjem opcije „ograničeni način rada”. Kako bi se to učinilo, potrebno se registrirati na YouTube - registracija je besplatna. Na dnu prozora pojavit će se alatna traka i opcija za uključivanje „ograničeni način rada”. Kako niti jedan filter nije apsolutno pouzdan potrebno je nadzirati dijete dok pretražuje video sadržaje, pogotovo ako je riječ o maloj djeci. Svakako provjerite jeste li prijavljeni na YouTube i je li opcija „restricted mode” uključena prije nego što djetetu prepustite da samo bira video sadržaj.

Ne objavljujmo video pod osobnim imenom - možemo izmisliti nadimak za svoj kanal!

Razmišljate li o tome promiču li youtuberi koje pratite lijepo ponašanje i etičke vrijednosti ili neprikladnim jezikom promiču nasilje, diskriminaciju, zlostavljanje?



Video igre - koju igru igraš?

Igranje igara je super zabavno, ali ponekad se možeš previše zagrijati za njih. To vremenski nekontrolirano igranje zove se ovisnost o video igrama i nije nimalo fora. Koliko si puta na lijep i sunčan dan izabrao videoigre umjesto igre na otvorenom s prijateljima?

Ovisnost o igrama je prisutna kad ne možeš prestati igrati čak i ako imaš nastavu, druge obveze i izbjegavaš prijatelje. Igre ti postaju najvažnija stvar na svijetu, a sve ostalo daleko je iza. Takva posvećenost igrama izaziva probleme u koncentraciji, odražava se na školskim ocjenama, uzrokuje probleme s mentalnim zdravljem, pretilost i druge zdravstvene probleme te probleme u druženju s prijateljima.

Važno je igrati umjereno, znati koliko je bitna tjelesna aktivnost, obrazovanje, vrijeme provedeno s prijateljima offline i druge brojne, zdrave i zabavne aktivnosti. Znakove ovisnosti o igrama važno je prepoznati na vrijeme i potražiti pomoć.

Pazi da igre ne preuzmu kontrolu nad tvojim životom!



Uloga influencera - kad narastem biti ću influencer!

Jeste li ikad pomislili kako je lijep taj posao influencera i kako bez puno truda, učenja i discipline možete zaraditi bogatstvo, dobiti pohvale, steći popularnost, karijeru i publiku? Važno je znati kako i uspjeh influencera zahtijeva trud, autentičnost i odgovornost.

Iza velikog broja influencera, kojima se divite i koje pratite, stoji mnogo truda i odgovornosti prema svojoj publici, posebno mlađim pratiteljima, mnogo rada i uloženog novca. Konkurencija je jako velika pa ni taj posao ne uspijeva tako lako svima.

Utjecaj na druge treba koristiti na pozitivan način, no razlikujete li vi dobar utjecaj od lošeg?



Primjer dobrog utjecaja influencera: Zamislite Luku i Leu koji su strastveno posvećeni svojim obvezama prema školi, nogometu, plesu i šminkanju. Oni na internetu svojim pratiteljima dijele iskustvo organiziranja vremena između škole, sportskih aktivnosti i istraživanja kreativnosti sa šminkom. Njihove objave motiviraju vas da se trudite u školi, uživate u sportu i izrazite svoju ljepotu na svoj, jedinstven način.

Primjer lošeg utjecaja influencera: S druge strane, postoje Ivan i Petra koji zanemaruju školu, promoviraju ljenčarenje i pretjerano korištenje šminke kao zamjenu za samopouzdanje. Praćenje takvih influencera može vas potaknuti na loš izbor prioriteta i nerealna očekivanja o ljepoti. Važno je uravnotežiti sve aspekte svog života.



Zamke na društvenim mrežama!!!

Catfishing: na internetu se skrivaju ljudi s lažnim identitetima. Nikad ne znate tko se krije iza ekrana. Budite oprezni i ne dijelite osobne informacije!

Cyber grooming: ponekad postoje odrasle osobe koje vas kontaktiraju na internetu i imaju loše namjere. Ne dopuštajte im da vam se približe!

Outing: predstavlja situacije kada netko bez dopuštenja iznosi informacije o seksualnoj orijentaciji ili rodnom identitetu osobe koja vam je poklonila povjerenje. Čuvajte svoju i tuđu privatnost!

Flaming: oblik neprijateljskog ponašanja na društvenim mrežama kada se upućuju agresivni ili uvredljivi komentari i poruke kako bi se drugu osobu uzrujalo ili je se uvuklo u raspravu. Morate biti svjesni da takvo ponašanje može nanijeti štetu te da su posljedice veće od onih koje možete zamisliti (traume i kaznena odgovornost)!

Fraping: nadamo se da do sada niste dijelili svoje lozinke sa „BFF“ jer uvijek je moguća situacija kada se povjerenje zloupotrijebi. Na taj način može se iskoristiti vaše ime, fotografije i slično u namjeri pisanja neprimjerenih komentara i poruka umjesto vas.

Zašto se čuvati?

Jer online svijet može biti pun opasnosti, a vaša sigurnost je najvažnija.

Kako reagirati?

Ako primijetite takve situacije ili se osjećate nelagodno, odmah obavijestite roditelje ili skrbnike. Ne biste trebali prolaziti kroz to sami.



Google Play zamke!

Google Play je *online* trgovina u kojoj kupujemo aplikacije, glazbu, filmove i još mnogo toga, a za kupnju sadržaja zajedno s roditeljima obrati pažnju na zamke i mogućnosti.

Kako bi koristili Google Play, potrebno je imati uređaj i Google adresu e-pošte. Sadržaj se može kupiti plaćajući kreditnom/debitnom karticom ili putem telefonskog računa. Suradnjom s operatorima i roditeljima, sadržaj se može platiti i preko korisničkog računa i tako izbjeći unošenje podataka o kartici.

Nakon uspješne kupnje, primit ćete potvrdu na adresu e-pošte koju ste naveli. Važno je uključiti “Provjere autentičnosti” kako biste spriječili neovlaštene kupnje.

Za povrat igara ili aplikacija dostupna su vam dva sata od trenutka kupnje. Otvorite Google Play i idite na “Račun” i “Povijest narudžbi” kako biste zatražili povrat. Maksimalni iznos za kupnju u Google Play-u je 49,77 €, a ukupni mjesečni iznos je 66,36 €. Možete postaviti mjesečni proračun i “Roditeljski nadzor” kako biste ograničili korištenje.

9. Umjetna inteligencija (AI)

Umjetna inteligencija (AI) je tehnologija koja računalima omogućuje razmišljanje, rješavanje problema i učenje poput ljudi. AI ima mnoge prednosti i njena primjena može povećati produktivnost, preciznost i brzinu rješavanja problema, a omogućava i personalizaciju te prilagodbu specifičnim situacijama i ljudima koji ju koriste. Predviđa se da će umjetna inteligencija donijeti goleme promjene u budućnosti, no ona je već sada prisutna u našem svakodnevnom životu. Neke danas već uobičajene primjene AI prepoznajemo u pametnim asistentima i personaliziranim preporukama. Kako bi uživali u mogućnostima ove tehnologije, a istovremeno sačuvali svoju sigurnost i privatnost, upućujemo vas na odgovorno korištenje AI-ja. Računalo prima podatke, obrađuje ih i daje vam odgovore koje tražite.

Sigurno već na svom mobitelu koristite virtualne asistente kao što je Siri ili Google Assistant koje razumiju vaše glasovne upute i daju vam odgovore na pitanja, postavljaju podsjetnike, preporučuju knjige ili filmove na temelju vaših interesa te obavljaju mnoge druge zadatke.

Sustavi generativne umjetne inteligencije poput OpenAI ChatGPT-a, Google Bard-a i Anthropic Claude-a u stanju su „razumjeti“ tekstualni zadatak i na temelju njega napisati odgovor. Znači, mogu napisati esej na bilo koju zadanu temu ili pjesmu u stilu poznatih pjesnika, a mogu i razgovarati upi-



sivanjem teksta. Osim alata koji mogu generirati pisani tekst, razvijeni su i alati koji razumiju ljudski govor i temeljem njege mogu generirati slike (MidJourney, DALL-E), videe, ali i sam ljudski govor koji može zvučati gotovo identično kao da ga govori neka stvarna osoba, poput vašeg prijatelja ili nastavnika.

Važno je zapamtiti da i AI nosi potencijalne prijetnje, kao što su narušavanje privatnosti, utjecaj algoritama na percepciju svijeta, ovisnost o tehnologiji, a pokreću se i etička pitanja. Generativna AI može stvoriti sadržaj po zahtjevu bilo koga i moramo biti svjesni toga da sadržaj ne mora uvijek biti točan. Zloupotreba ovako stvorenog sadržaja može uključivati kreiranje lažnih vijesti, ali i stvaranje video ili audio snimke te fotografije nečega što se nikad nije dogodilo.

10. Što gubimo kad izgubimo mobitel?

U svojim mobitelima čuvamo „svašta nešto“ i ponašamo se kao da imamo vlastiti „digitalni dnevnik“ ispunjen fotografijama, filmićima, šalabahterima, uspomenama, podsjetnicima na rođendane i obveze. U naš džep stane pravi mali arhiv koji dokumentira naš život! Međutim, često se događa da nam se mobitel pokvari, izgubi ili ga jednostavno zamijenimo 😊 pa nam nedostaje taj arhiv.

Kako ne bismo sve to što nam je drago u nepovrat izgubili, savjetujemo zaštititi se na sljedeće načine:

- 1. Zaključavanje ekrana:** postavi zaključavanje ekrana s PIN-om ili otiskom prsta
- 2. Ažuriranje:** redovito ažuriraj softver i aplikacije kako bi povećao sigurnost

- 3. Backup podataka:** povremeno spremi važne podatke na *cloud*. U oblaku se čuvaju podaci i aplikacije te ti je omogućen pristup tvojim informacijama putem interneta s različitim uređaja. To znači da podaci nisu pohranjeni samo na lokalnom uređaju nego su dostupni bilo gdje i bilo kada.
- 4. Praćenje uređaja:** znaš li za aplikaciju „Pronađi uređaj“ koja ti omogućava lakši pronalazak ako ga izgubiš?
- 5. Oprez s aplikacijama:** preuzimaj aplikacije samo iz službenih trgovina i budi na oprezu ako se traži previše privola.
- 6. Antivirusni programi:** kako bi svoj mobitel zaštitio od virusa instaliraj antivirusni program.
- 7. Wi-Fi mreže:** ne spajaj se na nepoznate bežične Wi-Fi mreže jer ne znaš tko je „domaćin“ i što može napraviti s podacima prikupljenim iz tvog uređaja.



11. I za kraj!

Svi provodimo dio dana uz ekrane, no važno je imati na umu da pretjerano korištenje tehnologija može imati utjecaj na naše mentalno i fizičko zdravlje, kao i na naše emocionalno stanje. Prekomjerno korištenje (više od dva sata dnevno) uzrokuje:

1. **Pad inteligencije:** previše gledanja u ekrane djeluje na našu koncentraciju i kreativnost te smanjuje oštrinu uma
2. **Fizičke promjene:** premalo tjelesne aktivnosti i lošeg položaja tijela zbog korištenja ekrana dovodi do debljanja, manjka energije i ostalih loših utjecaja na naše tijelo
3. **Promjene u raspoloženju:** previše vremena pred ekranima može nas učiniti anksioznima, neraspoloženima i razdražljivima, što utječe na naše emocionalno zdravlje

Održavanje ravnoteže između virtualnog i stvarnog svijeta može pomoći sačuvati našu inteligenciju, zdravlje i sretne emocije. Zato, neka ekrani budu dio, ali ne i najvažniji dio tvog života!



Roditelji i nastavnici, potrebno je svakodnevno upozoravati mlade da ograniče vrijeme pred mobilnim uređajima i ukazivati im na:

1. **Očuvanje zdravlja:** dugotrajno gledanje ekrana može štetiti očima, mentalnom zdravlju i tijelu. Nema pregovaranja o tome!
2. **Poticanje odgovornosti:** ukoliko djeca žele biti odgovorni prema sebi, postavite stroge granice i inzistirajte da ih se pridržavaju!
3. **Učenje prioriteta:** svakodnevno ih podsjećajte da su škola, tjelesna aktivnost, druženje s obitelji i prijateljima najvažniji, a mobilni uređaji nisu prioritet!
4. **Prevenција ovisnosti:** budite spremni na vrijeme reagirati ukoliko uočite bilo kakvu opasnost ili ovisnost te se obratite za pomoć stručnim osobama!

Odgovornost je ključna, a vi ste ti koji morate postaviti granice i osigurati da ih se djeca pridržavaju. Budite uporni kako biste pomogli djeci da izgrade zdrav odnos s tehnologijom!

Za one koji žele naučiti više

Susretnica

Susretnica nije obična aplikacija, ona je tu da vam pomogne razumjeti kako pravilno komunicirati i pristupiti osobama s različitim vrstama invaliditeta.

Aplikacija pruža niz praktičnih primjera iz stvarnih životnih situacija, kao što su situacije na kolodvoru, ulazak u dizalo, prelazak ceste, parkiranje i mnoge druge.

Susretnica je pristupačna, što znači da je dostupna svima jer omogućuje simuliranje iskustva osoba s invaliditetom, pa možete bolje razumjeti prepreke s kojima se suočavaju. Ona pomaže da budete bolji i obzirniji prema osobama s invaliditetom u stvarnom svijetu i da razumijete izazove s kojima se suočavaju u svakodnevnom životu te se nadamo da će i vama pomoći u tome da budete odgovorniji i podržavajući građani.



Aplikacija Kviz

Ova aplikacija ima dva važna cilja.

Prvi cilj je informiranje o vašim pravima u svijetu internetskih tehnologija, posebno ako ste osoba s invaliditetom. Želimo da svi znaju svoja prava i kako ih ostvariti.

Drugi cilj je podizanje svijesti o preprekama s kojima se suočavaju osobe s invaliditetom prilikom korištenja interneta. To je bitno jer želimo da na internetu svi imaju jednake šanse i mogućnosti.

Dok rješavate Kviz, možete isprobati različite simulacije motoričkih, vizualnih i kognitivnih poteškoća kako biste bolje razumjeli kako se osjećaju osobe s invaliditetom prilikom korištenja tehnologija.

Također, ona nudi smjernice za *web* dizajnere kako bi internetske stranice bile prilagođene za korisnike s poteškoćama.

Aplikacija omogućava i prilagodbu izgleda stranica. Možete mijenjati boje, veličinu teksta i koristiti audio funkcije.

S Kvizom ne samo da ćete naučiti o pravima i preprekama na internetu, nego ćete i biti dio promjene, čineći internet boljim i pravednijim mjestom za sve nas!



Ako do sada niste čuli, znajte da CARNET i Suradnici u učenju izrađuju brošure i internetski sadržaj vezano uz zaštitu djece na internetu. Svakako vam savjetujemo da posjetite ove adrese jer na njima se nalaze brojni odgovori na vaša

pitanja, ali i savjeti koji vam mogu pomoći. Na posljednjoj se može vidjeti i hrpa informacija o prvom hrvatskom satelitu koji će dvije godine provesti u svemirskim prostranstvima 😊



Sigurna knjižica



CERT infografike



Učitelji hr-obrazovni sadržaji



Crocube



Cybersecurity Ninja



Suradnici u učenju: **Društvena igra „Budi internet genijalac“** – u potrazi za boljim internetom “

Hrvatska regulatorna agencija za mrežne djelatnosti
Ulica Roberta Frangeša-Mihanovića 9, 10110 Zagreb
01/700 70 07, www.hakom.hr, zastita-djece@hakom.hr

Ova brošura prvenstveno je namijenjena roditeljima i njihovoj djeci u osnovnoj školi, ali može biti koristan izvor informacija svakomu tko želi više znati o temi ponašanja i sigurnosti djece na internetu. Brošura je rezultat suradnje HAKOM-a i Ministarstva znanosti i obrazovanja. Godina proizvodnje: 2024.