
Klikni, ali pazi!
Kako se zaštititi u svijetu interneta i pokretnih uređaja
HAKOM
HRVATSKA REGULATORNA AGENCIJA
ZA MREŽNE DJELATNOSTI

Dragi učenici, nastavnici i roditelji…

Što nam statistika govori o našim navikama na internetu?

Tijekom 2024. godine 40 posto djece u Hrvatskoj provodilo je više od tri sata dnevno na društvenim mrežama, a tijekom vikenda dnevno i 62 posto, dok 1,6 posto djece pokazuje simptome ovisnosti o društvenim mrežama. Istražena je i zastupljenost aktualnih emocionalnih problema kod djece, koji mogu biti uzrok i posljedica pretjeranog korištenja digitalnih tehnologija.

Trenutačno oko 7 posto učenika doživljava ozbiljne ili ekstremno ozbiljne simptome tjeskobe, depresivnosti i stresa, što su zabrinjavajući rezultati jer to djecu čini ranjivijima i u virtualnom okruženju te ukazuje na nužnost daljnjeg preventivnog djelovanja.

https://www.erf.unizg.hr/novosti?@=6g0r

Što mislim da znam, a što još moram naučiti?!

Roditelji nas u stvarnom svijetu uče jako bitnim stvarima kao što je vožnja biciklom, prelaženje ceste, korištenje pribora za jelo ili prepoznavanje opasnosti u prometu. Ali kad dobiješ svoj prvi mobitel, sve je nekako drugačije. Većina roditelja tada misli da znaš što radiš jer si s tehnologijom odrastao i sve ti to ide kao od šale. I stvarno, brzo svladaš nove aplikacije, znaš napraviti video, poslati poruku ili pronaći što god želiš.

No, ono što ti možda nitko nije pokazao jest kako biti siguran na mreži, kako prepoznati opasnosti, zaštititi svoje podatke i znati kad nešto „ne štima“. Kao što te roditelji nauče paziti u prometu, tako je važno naučiti i pravila sigurnosti u digitalnom svijetu jer i internet ima svoja raskrižja, semafore i nepredvidive vozače.

Zato vam želimo skrenuti pažnju na nekoliko stvari:

- Pokretni uređaj, tablet ili prijenosno računalo je alat, poput bicikla, olovke ili lopte – koristite ih po potrebi, a ne stalno (što s pokretnim uređajem često nije slučaj).
- 58 posto osoba provjerava svoj pokretni uređaj svakih sat vremena, što smanjuje koncentraciju, oduzima vrijeme za učenje i može stvoriti ovisnost.
- Vrijeme koje provodite u digitalnom svijetu je vrijeme u kojem ste sami odgovorni za svoje postupke, jer roditelja nema da vas nadziru ili zaštite.
- Baš kao što ne biste dijelili osobne podatke ili novac s nepoznatom osobom u stvarnom svijetu, isto vrijedi i na internetu – budite oprezni kome i što otkrivate!

Sloboda na mreži nosi i odgovornost. Pravila koja vrijede u stvarnom svijetu, vrijede i u digitalnom. Stoga budite pažljivi, promišljeni i sigurni.

HAKOM je državna agencija koja, uz mnoge druge važne zadaće, brine i o sigurnosti djece na internetu. Naš cilj je pomoći vam da naučite kako se odgovorno i sigurno ponašati u digitalnom svijetu u koji ulazite dok surfate, igrate se, učite, razgovarate, šaljete poruke ili objavljujete sadržaj na društvenim mrežama.

Za pristup svijetu elektroničkih komunikacija potrebni su nam operatori (znate li koji je vaš?), kojima plaćamo uslugu, bilo putem mjesečnog računa ili putem unaprijed plaćene usluge (bonova). HAKOM nadzire te operatore i brine da ispunjavaju zakonske obveze prema svojim korisnicima, odnosno svima nama koji koristimo elektroničke komunikacijske usluge.

Svake godine u veljači HAKOM u suradnji s partnerima obilježava Dan sigurnijeg interneta, koji se istovremeno obilježava u čak 140 država svijeta sa ciljem promicanja sigurnijeg i odgovornijeg korištenja tehnologija. Upravo zato ova brošura sadrži niz savjeta, informacija i uputa koje će „malima i velikima“ pomoći u daljnjem razvoju digitalne pismenosti.

Pa stoga krenimo zajedno ☺!

Osobni podatci - zašto su bitni?

Što su osobni podatci, kako ih zaštititi u digitalnom svijetu ?

Osobni podatci su svi podatci koji se odnose na tebe kao pojedinca i na temelju kojih te se može identificirati. To su, primjerice, ime i prezime, adresa, OIB, broj osobne iskaznice, adresa elektroničke pošte, telefonski broj. Ali, djelomično, i IP adresa (svi znamo što je to ☺), lokacija, kolačići na internetu, identifikatori vašeg uređaja. Postoje i osjetljivije kategorije podataka kao što su zdravstveni i biometrijski podatci, koji se obično dodatno štite naprednijim mehanizmima.

Zašto bi netko htio ukrasti moje osobne podatke? Što s tim može napraviti?

U digitalnom svijetu podatci imaju konkretnu vrijednost. Ako zlonamjerne osobe dođu do njih, mogu ih iskoristiti za prijevare, krađe identiteta odnosno lažno predstavljanje, ali potencijalno i pristup svim vašim aplikacijama. Zato su osobni podatci danas vrijedni gotovo kao novac, a nekad i više jer se različite prevare mogu izvesti kada netko zna puno o tebi.

Koje su najčešće prijevare vezane uz osobne podatke? Kako mogu prepoznati sumnjive poruke?

- phishing, odnosno poruke u kojima se netko lažno predstavlja. Te poruke izgledaju kao da dolaze od banke, dostavne službe ili čak vaših prijatelja, a traže da kliknete na poveznicu i upišete osobne podatke
- lažne internetske trgovine
- krađe putem oglasnika (kupovina i prodaja)

Kada nas netko traži da hitno odgovorimo na poruku, ažuriramo podatke na poveznici ili da odmah kliknemo, pošaljemo ili instaliramo – to može biti znak da nešto nije u redu, odnosno da je u pitanju prijevara.

Također, ako dobiješ obavijest o prijavama na račune koje nisi kreirao – treba reagirati.

Veliki je rizik kada svoje podatke unosiš na stranicama ili u aplikacijama koje nisu provjerene. Pokušaj to uvijek učiniti zajedno s roditeljima!

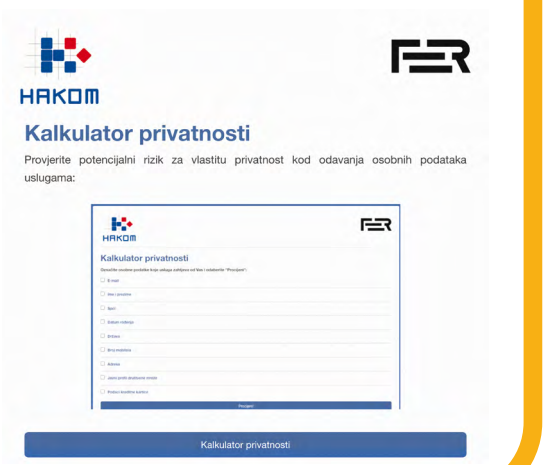
Savjet za roditelje: Najvažnije je graditi povjerenje i povremeno zajedno s djetetom pregledati uređaje, aplikacije i postavke privatnosti. Postavljanje pitanja djetetu nije kontrola, nego jačanje sigurnosti. Poruka koju djeca najbolje prihvaćaju dolazi uz razgovor, a ne uz predstavljanje zabrane.

Savjet za čuvanje osobnih podataka:

- Ne dijelite podatke ako ne znate tko ih prikuplja i zašto.
- Pazite što instalirate na svoj pokretni uređaj.
- Razmislite prije nego nešto podijelite.
- Ne koristite iste lozinke na više mjesta.
- Koristite višefaktorsku autentifikaciju gdje god možete.
- Provjeravajte postavke privatnosti na društvenim mrežama.
- Budite kritični uvijek kad se traže vaši osobni podatci.
- I naravno, koristite Kalkulator privatnosti ☺.

UPOZNAJ SE S APLIKACIJOM KALKULATOR PRIVATNOSTI

kako bi provjerio potencijalni rizik koji nastaje pri ostavljanju osobnih podataka na internetu putem našeg kviza, u sklopu kojega se nalazi i Kviz o sigurnosti na internetu, koji vas upoznaje s najčešćim prevarama na internetu.



TVOJA LOZINKA

Provjeri koliko te štiti tvoja lozinka! Idealna lozinka ima što više znakova (to je jako bitno), sadrži velika i mala slova, interpunkcijske znakove i poneki broj. Budi kreativan u njezinu osmišljavanju, ali pazi da se ne ponavljaš jer pravilo je da na raznim mjestima NE koristimo istu lozinku.

Ne dijeli lozinku, čak ni s BFF-om jer može iskoristiti tvoje ime, fotografije i slično u namjeri pisanja neprimjerenih komentara i poruka.

Ako živiš u Zadru, zoveš se Jelena i imaš 11 godina, a lozinka ti je Jelena11, a nickname ti je JeleZD misliš li da je sigurna? J11@_ZDozk?@!" mnogo je sigurnija, no teža za zapamtiti. Samo pazi da ju i zapamtiš 🙂!

Ako želiš provjeriti koliko si online siguran i kreativan na poveznici www.howsecureismypassword.net možeš to i saznati.

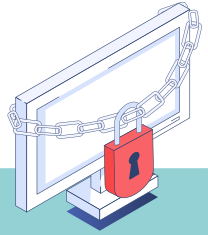
I ONDA SE ČUDE KAKO...

Nevjerojatno. Lozinka za video nadzor Louvrea bila je 'Louvre'

Upoznaj se s antivirusnom zaštitom

Maliciozni programi poput crva i trojanskog konja pokušavaju doći do naših osobnih podataka koji su pravo zlato za hakere. Zato budimo oprezni i koristimo i redovito ažurirajmo antivirusnu zaštitu jer u protivnom ona nas neće moći štititi koliko bi trebala.

Znaš li da se dnevno u cyber prostor „pusti“ preko 3000 novih malicioznih programa pa je ažuriranje ključno? Zatooo, briši aplikacije koje više ne koristiš!



PRIJE NEGO ŠTO OSTAVIŠ TRAG SAZNAJ ŠTO SU TO „KOLAČIĆI“!

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. Prihvati samo nužne kolačiće, a ne sve, ne ostavljaj više digitalnih tragova nego što trebaš.

Kolačići mogu biti problematični jer prateći tvoje aktivnosti na internetu i skupljajući informacije o tome koje stranice posjećuješ i što te zanima, najčešće te podatke koriste za ciljano oglašavanje, bez tvoje jasne suglasnosti.

Ako se pitaš zašto ti se na internetu prikazuje sadržaj koji odgovara tvojim interesima, razlog tomu su kolačići. Oni prate tvoje aktivnosti i šalju ti ciljano sadržaj koji te zanima.

DIGITALNI TRAG - OSTAJE DUŽE NEGO ŠTO MISLIŠ

Digitalni trag je sve ono što ostavljaš iza sebe na internetu, svjesno ili nesvjesno. To su fotografije, komentari, lajkovi, pretrage pa čak i vrijeme koje provodiš gledajući video. Na primjer, kad lajkaš objavu, aplikacija bilježi ne samo lajk, već i koliko si dugo gledao, gdje si bio i koji uređaj koristiš. Algoritmi analiziraju što gledaš i što preskačeš. Te informacije se prikupljaju, analiziraju i dalje upotrebljavaju. Internet nije samo ono što vidiš. Većina podataka nalazi se ispod površine, tamo gdje trag ne nestaje. Površina su profili i objave, ali duboko ispod ostaju obrasci, navike, kontakti... Ti podatci se spajaju u tvoj digitalni profil, koji može otkriti tvoje interese i navike.

Tvoj digitalni trag ne nestaje, on raste svakim tvojim klikom.

Savjet:

- provjeri postavke privatnosti na aplikacijama – npr. isključite lokaciju na fotografijama
- koristi jake lozinke i dvofaktorsku autentifikaciju
- razmisli prije objave: ako ne želiš pokazali sliku nepoznatoj osobi, nemoj ju dijeliti online

Savjet za roditelje:

Sadržaji koji su danas bezazleni za nekoliko godina mogu postati problem. Djeca oblikuju vlastiti digitalni trag, ali roditelji mu trebaju dati smjer i biti primjer. Roditelji nisu i ne smiju biti samo promatrači, već odgovorni vodiči. Prema Obiteljskom zakonu roditelji su dužni štititi dijete i u digitalnom prostoru.

Najvažnije je razgovarati! Bez straha i bez zabrana. Djeca trebaju znati da digitalni svijet ne zaboravlja i zato svi zajedno naučite štititi svoje podatke!

UI, ALGORITMI I SINTETIČKI MEDIJI

Zamisli da ti netko kaže: „Imaš 25 godina koje moraš provesti gledajući u mobitel.“

Zvuči nevjerojatno, zar ne?

Ali prosječna osoba danas provede više od pet sati dnevno na ekranu, a studenti čak više od šest sati. Kad se sve to zbroji, ispadne da tehnologiji poklonimo gotovo 28 godina života!

To je vrijeme koje bismo mogli provesti vani, s prijateljima, u igri, smijehu i stvarnom životu. I sada nam je već prilično jasno, tehnologija je korisna i zabavna, ali pravi život događa se izvan ekrana u trenucima koje ne možemo “skrolati” natrag!

Znaš li tko ti zapravo „priča“ s ekrana? Možda misliš da je to pravi čovjek, ali ponekad to uopće nije tako. **Umjetna inteligencija** danas može stvoriti fotografije, video zapise i glasove koji izgledaju potpuno stvarno, iako u stvarnosti ne postoje. To se zove **sintetički medij**.

Zamisli video u kojem tvoj omiljeni pjevač govori nešto što nikada nije rekao. Izgleda stvarno, pokreti su prirodni, glas savršen, ali cijeli video stvorio je računalni program. To se zove **deepfake**. I iako može biti zabavno, zna biti i opasno, jer takvi sadržaji mogu širiti lažne vijesti ili zavarati ljude.

Još zanimljivije (i pomalo čudno) – umjetna inteligencija ponekad može **“halucinirati”**. To znači da izmišlja stvari koje zvuče pametno i uvjerljivo, ali nisu istinite. Kao kad bi ti prijatelj samouvjereno ispričao priču koja se nikad nije dogodila.

A znaš tko često odlučuje što ćeš vidjeti na ekranu?

To su **algoritmi**, pametni programi koji prate što gledaš, što ti se sviđa, što lajkaš i na čemu se zadržavaš.

Na temelju toga odlučuju što će ti sljedeće pokazati jer žele da što duže ostaneš online.

Zato ponekad imaš osjećaj da ti internet "čita misli" jer algoritmi uče o tebi iz tvojih klikova.

Zato je važno da znaš prepoznati razliku između stvarnog i generiranog. Kad nešto vidiš na internetu, nemoj odmah povjerovati. Zastani, provjeri i razmisli. Umjetna inteligencija može biti super alat za učenje i zabavu, ali samo ako ti kontroliraš nju, a ne ona tebe.

Savjet:

Koristi umjetnu inteligenciju pametno, uči, istražuj i zabavljaj se, ali uvijek razmišljaj i provjeri što je istina! Umjetna inteligencija može pomoći da budeš kreativniji i pametniji, ali ti si taj koji odlučuje kako ju koristiti na dobar način.

A JESI LI SE KORISTIO CHATBOTOVIMA KADA TRAŽIŠ ODGOVORE NA NEKA PITANJA?

Vjerujemo da ti je poznato kako je chatbot računalni program koji razgovara s ljudima pomoću teksta ili glasa. Može odgovarati na tvoja pitanja, pomagati u rješavanju problema ili voditi razgovor, baš kao da pričaš s nekom osobom.

👩 Korisnik: Bok! Trebam pomoć oko zadaće.

🤖 Chatbot: Naravno! O kojoj se temi radi?

👩 Korisnik: O umjetnoj inteligenciji.

🤖 Chatbot: Super! Umjetna inteligencija je tehnologija koja uči i razmišlja poput ljudi.

MEMOVI, JESU LI TI ZANIMLJIVI?

Zamisli da skrolaš po TikToku ili Snapchatu i naiđeš na onaj savršeni mem, smiješan, točan i baš te „pogodi“. Pošalješ ga frendu, on podijeli dalje i odjednom ga svi vide. Jesi li ikad razmišljao zašto baš taj mem vidiš?

Memovi nisu samo šale, oni prenose poruke, oblikuju mišljenje i ponekad šire stereotipe ili lažne informacije. A iza svega stoje algoritmi, programi koji prate što voliš i pokazuju ti sadržaj koji će izazvati emociju.

Zato, kad vidiš mem koji te nasmije ili naljuti, zastani i razmisli: što mi zapravo poručuje i zašto ga vidim? Kad razmišljaš kritički, ti kontroliraš memove, ne oni tebe!

Savjet za roditelje:

Razvoj umjetne inteligencije napreduje tolikom brzinom da se mnogi roditelji osjećaju izgubljeno. No, ne morate znati sve, dovoljno je da razumijete osnove, postavljate prava pitanja i znate gdje trebate potražiti pomoć. Evo nekoliko korisnih smjernica:

1.

Razgovarajte s djecom o umjetnoj inteligenciji. Pitajte ih znaju li što je AI, koriste li alate poput ChatGPT-a ili drugih chatbotova. Djeca vole istraživati i isprobavati nove stvari, važno je da to rade uz vaš nadzor i razgovor.

2.

Vježbajte prepoznavanje sintetičkih sadržaja. Zajedno istražite stranice poput Which Face Is Real? ili alate koji otkrivaju deepfake videa. Naučite djecu kritički gledati digitalne slike i videa.

3.

Učite ih provjeravati informacije. Ako koriste AI za školu ili učenje, objasnite im da odgovori nisu uvijek točni. Pomozite im razlikovati pouzdane izvore od onih koji to nisu.

4.

Provjerite alate koje koriste. Neki AI alati imaju dobna ograničenja ili prikupljaju podatke. Provjerite jesu li sigurni i primjereni dobi vašeg djeteta.

5.

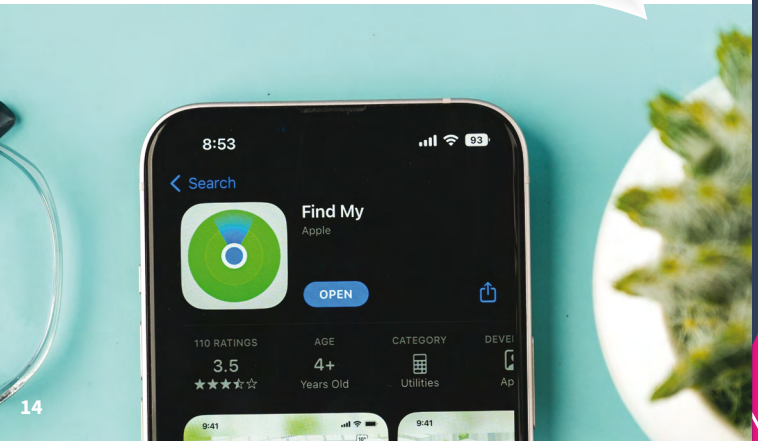
Razgovarajte o algoritmima i personalizaciji sadržaja. Objasnite da sadržaj koji vide nije slučajan – algoritmi biraju što će im se prikazati. Potaknite ih da aktivno traže informacije, a ne samo „skrolaju“.

6.

Budite primjer. Djeca uče promatrajući odrasle. Ako vi promišljate o onome što gledate i dijelite online i oni će naučiti isto.

Ukratko: ne morate biti tehnološki stručnjak. Najvažnije je da ste uključeni, otvoreni za razgovor i spremni učiti zajedno s djecom.

ŠTO GUBIMO KAD IZGUBIMO POKRETNI UREĐAJ?



U svojim pokretnim uređajima čuvamo „svašta nešto“ i oni su nalik na naš osobni „digitalni dnevnik”, ispunjen fotografijama, filmićima, šalabahterima, uspomenama, podsjetnicima na rođendane i obveze putem kalendara.

U naš džep stane pravi mali arhiv koji dokumentira naš život!

Međutim, često se događa da nam se pokretni uređaj pokvari, izgubi ili dobijemo novi pa nam taj dnevnik nedostaje.

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

1. Zaključavanje ekrana: postavi zaključavanje ekrana s PIN-om, otiskom prsta odnosno s Face-ID-om.

2. Ažuriranje: redovito ažuriraj softver aplikacije kako bi zadržao sigurnost.

3. Backup podataka: povremeno spremi važne podatke u oblak (cloud). U oblaku se čuvaju podaci i aplikacije te se omogućava pristup tvojim informacijama putem interneta s različitih uređaja. To znači da podaci nisu pohranjeni samo na lokalnom uređaju, već su dostupni bilo gdje i bilo kada.

4. Praćenje uređaja: Znaš li za aplikaciju „Pronađi uređaj“ koja ti omogućava da ga lakše pronađeš ako ga izgubiš?

5. Oprez s aplikacijama: preuzimaj aplikacije samo iz službenih trgovina i pazi koje sve dozvole traže.

6. Antivirusni programi: kao što smo već u tekstu naveli.

7. Wi-Fi mreže: ne spajaj se na nepoznate Wi-Fi mreže jer ne znaš tko je „domaćin“ i što može napraviti s podacima prikupljenim iz tvog uređaja.

DSA

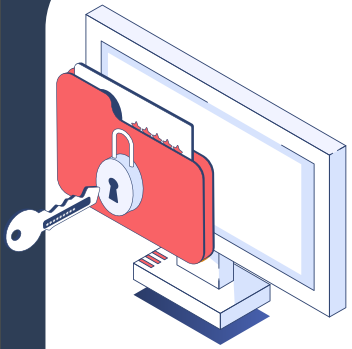
Svi bismo se na internetu trebali osjećati sigurno, bez sadržaja i ljudi koji nas plaše, ljute ili nam smetaju.

Zato postoji DSA, odnosno Akt o digitalnim uslugama, koji postavlja jasna pravila ponašanja velikih platformi na internetu.

On omogućuje svima pa i tebi, prijavu sadržaja koji je nezakonit ili jednostavno ne bi trebao biti na mreži. Zbog tih pravila, aplikacije koje svakodnevno koristiš poput Snapchata, YouTubea, Instagrama ili TikToka, sada imaju nova sigurnosna pravila.
Također, više se ne smiju prikazivati oglasi posebno usmjereni na djecu, a računi korisnika mlađih od 16 godina na TikToku i YouTubeu automatski postaju privatni, tako da njihove objave mogu vidjeti samo prijatelji.

Zabranjeni su i takozvani „tamni obrasci“, trikovi u dizajnu stranica koji te pokušavaju nagovoriti da klikneš, kupiš ili se pretplatiš na nešto što ti zapravo ne treba.

Takvi trikovi često su skriveni kako bi te zadržali što dulje online.



Savjet:

Mnoge su aplikacije napravljene tako da te “uvuku” i ne puste. Pobijedi sustav tako što ćeš isključiti ekran, otići van i uživati na drugačiji način. Istraživanja pokazuju da što više vremena provodiš online, to ti razina sreće postaje manja!

APLIKACIJA SUSRETNICA!

Do sada smo naučili kako se zaštititi na internetu, prepoznati lažne oglase, prijaviti neprikladan sadržaj i ne dopustiti da nas aplikacije zavaraju.

Ali važno je znati kako biti pažljiv i u stvarnom svijetu, ne samo online.

Iz tog razloga smo izradili aplikaciju Susretnica koja te uči kako se ponašati prema osobama s invaliditetom u stvarnom životu.

Kroz zanimljive primjere iz svakodnevnog života poput ulaska u dizalo, prelaska ceste ili kupnje karte, pokazuje ti kako pomoći osobama s invaliditetom na pravi način.

Najvažnije pravilo je - uvijek pitaj treba li pomoć prije nego što pomogneš!

Tako pokazuješ poštovanje, razumijevanje i dobrotu, osobine koje vrijede i na internetu i izvan njega.

Skeniraj QR Susretnice i otkrij kako male geste mogu promijeniti nečiji dan!

Dobrodošli u aplikaciju za podizanje svijesti o svakodnevnoj komunikaciji s osobama s invaliditetom!

Ova aplikacija razvijena je s ciljem edukacije o ispravnom postupanju prilikom susreta s osobama s invaliditetom te poticanja ljudi na kontakte bez straha.

DRAGI RODITELJI, ZA KRAJ IMAMO I PAR UPUTA ZA VAS!

U digitalnom svijetu roditelji imaju važnu ulogu pomoći djeci da sigurno rastu, istražuju i uče, a pritom ostanu zaštićeni od neprimjerenih sadržaja. Zato postoje i pravila koja pomažu upravo vama.

Prilikom sklapanja ugovorne obveze za uslugu kojom će se koristiti vaše dijete, operatori javno dostupnih elektroničkih komunikacijskih usluga dužni su ponuditi mogućnost zabrane pristupa sadržajima koji nisu namijenjeni djeci, ako za to postoji tehnička mogućnost.

Pri potpisivanju ugovora operator ili prodavač mora vam ponuditi tu opciju, a možete je uključiti ili isključiti bilo kada tijekom trajanja ugovora.

Ako zaprimite SMS ili MMS poruke s neprimjerenim sadržajem možete ih prijaviti svom operatoru ili poslati obavijest na adresu: nezeljeni.sms@hakom.hr. Takvi će brojevi, nakon provjere, biti blokirani u najkraćem mogućem roku.

Također, možete besplatno zatražiti zabranu slanja ili primanja poruka s posebnom tarifom (brojevi 6xx xxx, 8xx xxx i slično).

Postoji i mogućnost postavljanja ograničenja potrošnje u minimalnom iznosu od 7,00 eura nakon ugovorene mjesečne naknade kako biste zadržali kontrolu nad troškovima.

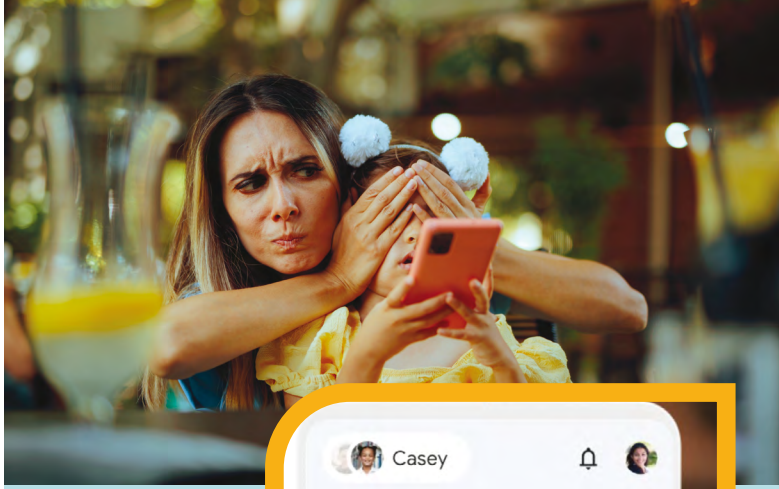
Ako koristite televizijske usluge, imajte na umu da svi operatori omogućuju roditeljsku zaštitu. Njome možete ograničiti gledanje neprimjerenih sadržaja poput nasilnih ili pornografskih programa.

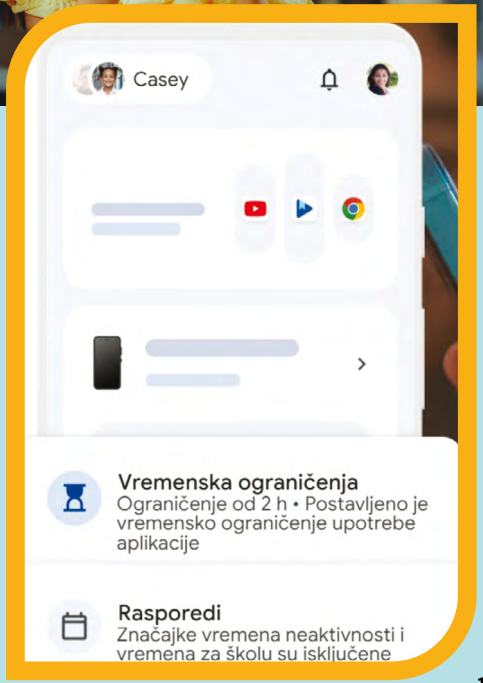
Kod mlađe djece preporučuje se korištenje **alata roditeljskog nadzora** (**primjerice Family Link ili Dinner Time**) i filtriranje sadržaja. Navedeni alati obiteljima pomažu u razvoju zdravih, pozitivnih digitalnih navika, poštujući njihove individualne odluke o upotrebi tehnologije. Pomoću jednostavnih alata možete provjeriti kako vaše dijete provodi vrijeme na svom uređaju, podijeliti lokaciju, upravljati postavkama privatnosti i pronaći najbolju ravnotežu za svoju obitelj.

Preporučljivo je i definirati:

- vrijeme koje dijete smije provesti pred ekranom,
- vrste igara i aplikacija koje koristi,
- doba dana u kojem su ekrani dopušteni.

No, jednako je važno da razgovarate s djecom o tim postavkama i objasnite im zašto postoje.





Obiteljski zakon, članak 95. stavak 4.

Roditelji imaju pravo, dužnost i odgovornost nadzirati dijete u njegovom druženju i komunikaciji, bilo uživo, bilo putem društvenih mreža ili drugih oblika elektroničke komunikacije te zabraniti kontakte koji nisu u skladu s dobrobiti djeteta.

Roditelji, imamo nekoliko prijedloga za vas:

- Sudjelujte s djecom u izazovu „Klik ili trik!!“
- Nakon izazova pročitajte brošuru o sigurnom internetu
- Upoznajte se s kvizovima HAKOM-a putem QR kodova
- Razmislite o roditeljskoj zaštiti i filtriranju sadržaja
- Posjetite internetske stranice operatora, vidjet ćete koliko korisnih i kreativnih inicijativa nude
- Budite potpora svojoj djeci jer i mi odrasli ponekad previše vremena provodimo online
- Sjetite se da prosječan razgovor roditelja i djeteta traje samo sedam minuta dnevno – pokušajte ga produžiti
- Za korisnička pitanja, uvijek možete posjetiti www.hakom.hr

Na HAKOM YoTube kanalu dostupni su i **webinari za roditelje o sigurnosti djece na internetu**, pogledajte ih kad stignete!

IZAZOV ZA SVE: KLIK ILI TRIK! 6,7,6,7,6…

Dragi svi, evo jednog zanimljivog zadatka za kraj!

Ponesite ovu brošuru kući i prolistajte je zajedno s roditeljima.

Razgovarajte, uspoređujte odgovore i vidite tko zna više o sigurnom internetu.

U školi potom podijelite dojmove na kojem pitanju je bio najveći TOP ili FLOP!

Najbolje učimo jedni uz druge!

✅

Tko je sve na tvom popisu prijatelja?

Provjeri imaju li tvoji roditelji na društvenim mrežama, među prijateljima, nepoznate osobe. Ako imaju, objasni im da si ti svoje izbrisao radi sigurnosti i zašto bi i oni trebali učiniti isto.

✅

Super lozinka!

Pohvali se roditeljima da si na stranici www.howsecureismypassword.net provjerio koliko je tvoja lozinka jaka. Zajedno provjerite i njihove lozinke, pokaži im kako ih napraviti dužima, pametnijima i sigurnijima.

✅

Kalkulator Privatnosti

Otvorite zajedno Kalkulator privatnosti i Kviz o sigurnosti na internetu (težina raste – od lagane do teške!). Ovaj put ti provjeri znanje svojih roditelja! Na kraju im daj ocjenu za rezultat, budi strog, ali pravedan.

✅

Deepfake detektiv

Pokaži roditeljima nekoliko deepfake videa ili fotografija. Objasni im što to znači i zašto takvi sadržaji mogu biti opasni. Nije sve što vidimo na internetu stvarno!

✅

TikTok razgovor

Imaju li tvoji roditelji TikTok? Pokaži im neke opasne izazove spomenute u brošuri. Objasni im zašto iako izgledaju zabavno, mogu biti štetni ili čak životno opasni. Pokaži roditeljima neka svoja videa ili objave s TikToka, Instagrama ili Snapchata. Razgovarajte o tome što bi bilo da te objave vidi netko tko te ne poznaje. Sada shvaćaš, objavljuješ samo ono što možeš pokazati i brižnim očima svojih roditelja!

6. Razgovor bez ekrana

Zamisli, prosječan razgovor roditelja i djeteta traje samo sedam minuta dnevno! Pokušajte zajedno produljiti to vrijeme bez pokretnih uređaja bez ekrana. Pričajte o školi, prijateljima, internetu, hobijima… Možda otkrijete da je pravi svijet zanimljiviji od virtualnog.

7. Algortimske “pogađalice”

Pitaj roditelje znaju li što su algoritmi, tko ih bolje razumije? Objasni im kako algoritmi „biraju“ što ćete vidjeti na YouTubeu, TikToku ili Googleu i kako je važno znati kad nas pokušavaju zadržati online.

Pamet u glavu, pamet u prste, na internetu imaj stavove čvrste.

Nemoj nikad davat svoje puno ime da zločesti ljudi ne okoriste se njime.

Sada ću ti otkriti jedan mali trik, umjesto punog imena izmisli si nick.

Nemoj cijele dane pred ekranom čubiti, vrijeme za druženje potpuno izgubiti.

U redu je gejmat, ali imaj mjeru, ne daj da te od ekrana glavobolje peru.

Nema ružnih riječi, vrijeđanja i hejta, vrijede ista pravila ko iz stvarnog svijeta.

Ponašaj se pristojno kada si na chatu, sve što radiš ružno na tvoju je štetu.

Ako ti se na chatu netko sumnjiv javi ne drži to za sebe nego starcima prijavi.

Bitno je da ne skrivaš kad te nešto muči, roditelj je tu da te zaštiti i nauči.

Pamet u glavu, pamet u prste, na internetu imaj stavove čvrste.

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, obrazovanja i mladih. Godina proizvodnje: 2026.