Ključevi sigurnog interneta

Kako se zaštititi u svijetu interneta i pokretnih uređaja

HAKOM
HRVATSKA REGULATORNA AGENCIJA ZA MREŽNE DJELATNOSTI

Dragi učenici, nastavnici i roditelji….
tko drži ključ vaše sigurnosti na internetu?

Priča o izgubljenom ključu

Jedne noći čovjek je tražio ključ ispod uličnog fenjera. Prolaznici su mu prilazili i pitali ga što traži.

„Tražim ključ" odgovarao je.

Pridružili su mu se, tražili su zajedno, no ključ nisu našli. Konačno su ga upitali: „Jesi li siguran da si ga baš ovdje izgubio?"

„Ne, izgubio sam ga kod kuće," odgovorio im je.

Prolaznici su zbunjeno upitali: „Pa, zašto ga tražiš ovdje?"

„Zato što je ovdje svjetlo," kazao je.

HAKOM je državna agencija čiji je zadatak (uz mnoge druge važne poslove) i zaštita djece u online okruženju.

Prvenstveno, HAKOM-ova zadaće je zaštita korisnika u svijetu elektroničkih komunikacija u koji ulazimo kada surfamo, igramo videoigre, pričamo, pišemo poruke, objavljujemo sadržaj na društvenim mrežama i slično.

Kako bi ušli u taj svijet potrebni su nam operatori (*znate li koji je vaš?)* kojima plaćamo uslugu putem mjesečnog računa temeljem ugovora ili putem unaprijed plaćene usluge (bonova).

HAKOM brine da operatori prema svojim korisnicima (*svima nama u svijetu elektroničkih komunikacija*) ispunjavaju obveze koje su im propisane.

Svake veljače HAKOM 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, uputa i novosti koje će „malima i velikima" pomoći u daljnjem razvoju digitalne inteligencije.

Ovogodišnju brošuru nazvali smo *Ključevi sigurnog interneta* jer kao što je čovjek tražio ključ na pogrešnom mjestu, mnogi od nas traže sigurnost na internetu na krivim mjestima ili očekuju da će drugi paziti na njih. No, ključ naše sigurnosti - u digitalnom svijetu - ipak je u našim rukama.

Pa stoga krenimo ☺

Znam da ništa ne znam

Roditelji nas u stvarnom svijetu uče kako voziti bicikl, prelaziti cestu, koristiti pribor za jelo. Ali, kad dobijete pokretni uređaj tomu najčešće ne prethodi nikakva priprema jer i vi i vaši roditelji smatrate kako ga znate samostalno koristiti. Vi ste vrlo snalažljivi kad je u pitanju surfanje internetom i tu ste ponekad i spretniji od roditelja, ali često vam nedostaje znanje o tome kako se zaštititi.

Zato vas želimo podsjetiti i ukazati vam kako:

- su pokretni uređaj, tablet ili prijenosno računalo **alati** poput bicikla ili olovke koje koristite po potrebi, a nemate ih stalno uz sebe (što vjerojatno nije slučaj s pokretnim uređajem)
- da 58 posto osoba provjerava svoj pokretni uređaj svakih sat vremena, što oduzima vrijeme za učenje, smanjuje koncentraciju i stvara ovisnost
- je vaša sigurnost u vremenu koje prevodite na mreži isključivo vaša odgovornost jer tada nisu prisutni roditelji koji će vas nadzirati i štititi

Sloboda uvijek nosi i odgovornost. Na internetu morate biti pažljivi jer pravila koja vrijede u stvarnom svijetu, vrijede i u onom digitalnom.

KLJUČEVI SIGURNOG INTERNETA

Zaključaj svoje osobne podatke (adresu e-pošte, ime i prezime, korisničko ime, lozinku, informacije o spolu, datumu rođenja, broju pokretnog uređaja, adresi, podacima s kreditne kartice) - oni su tvoj siguran prolaz u digitalni svijet!

ZAŠTITI SVOJE OSOBNE PODATKE

Ne predstavljaj se svojim pravim imenom (koristi *nickname*), ne otkrivaj adresu (isključi lokaciju), broj telefona i druge osobne podatke nepoznatim osobama na internetu.

Pogledaj svoje društvene mreže, provjeri popis prijatelja/pratitelja i pobriši sve one koje ne poznaješ.

Zašto? Zato što se na internetu skrivaju ljudi s lažnim identitetima i nikad ne možeš znati tko se krije iza ekrana i koje su mu namjere. Dovoljno je da nepoznati „prijatelj“ vidi tvoju lokaciju i time ugrozi tvoju sigurnost i sigurnost tvoje obitelji. Puno je slučajeva kada su takvi „prijatelji“ iskoristili situaciju na način da su zatražili novac ili slanje neprimjerene fotografije.

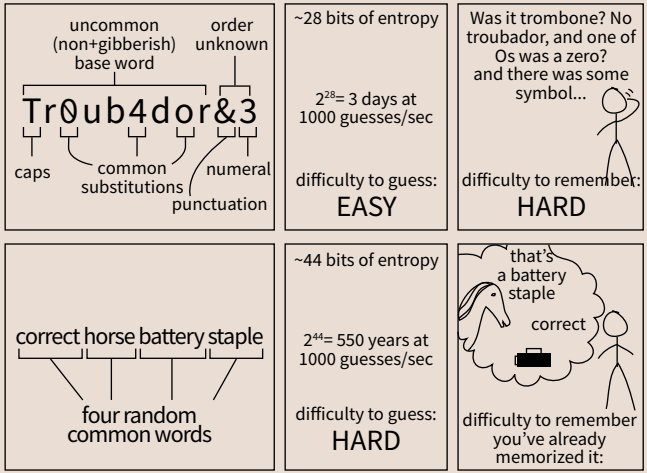
Provjeri potencijalni rizik odavanja osobnih podataka putem našeg kviza **Kalkulator privatnosti** u sklopu kojega se nalazi i **Kviz o sigurnosti na internetu** koji nas upoznaje s najčešćim prevarama na internetu**:**

Ne možeš zamisliti koliko je velik internet i što sve sadržava? Mislimo da bi ti u stvaranju predodžbe mogla pomoći slika ledenjaka.

Prije nego nastavimo dalje, predlažemo ti da obavezno riješiš Kalkulator privatnosti i provjeriš jesu li ti na aplikaciji Snapchat isključene lokacijske usluge (baci pogled na postavke privatnosti) jer jako je opasno baš svima dati informaciju gdje se nalazimo i to u svakom trenutku!

Provjeri koliko je snažna tvoja lozinka – idealna lozinka sadržava što više znakova (to je jako bitno) ima 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.

TVOJA LOZINKA

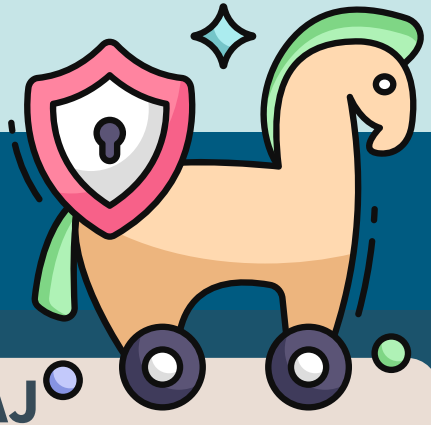


Through 20 years of effort, we've successfully traned everyone to use passwords that are hard for humans to remember, but easy for computers to guess.

Ne dijeli lozinku, čak ni s najboljim prijateljem jer može iskoristiti tvoje ime, fotografije i slične podatke u namjeri pisanja neprimjerenih komentara i poruka.

Ako živiš u Rijeci, zoveš se Lea i imaš 12 godina, a lozinka ti je LEA12, a nickname ti je LeaRI, misliš li da si sigurna? L3@_R!j3K@" mnogo je sigurnija, no teža za zapamtiti.

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



UPOZNAJ SE S ANTIVIRUSNOM ZAŠTITOM

Maliciozni programi poput crva i trojanskog konja pokušavaju doći do tvojih osobnih podataka koji su pravo zlato za hakere.

Zato trebamo biti oprezni te koristiti i redovito ažurirati antivirusnu zaštitu jer ako to ne činimo ona nas neće moći štititi koliko bi trebala.

Znaš li da se dnevno u virtualni prostor „pusti" preko 3000 novih malicioznih programa pa je ažuriranje ključno? Ujedno, briši aplikacije koje više ne koristiš.

Svakako briši aplikacije koje više ne koristiš.

POŽURI POLAKO - NE „KONZUMIRAJ“ SVE KOLAČIĆE

Većina kaže – yes to all!

Prihvati samo nužne kolačiće, a ne sve. Ne ostavljaj više digitalnih tragova nego što je potrebno.

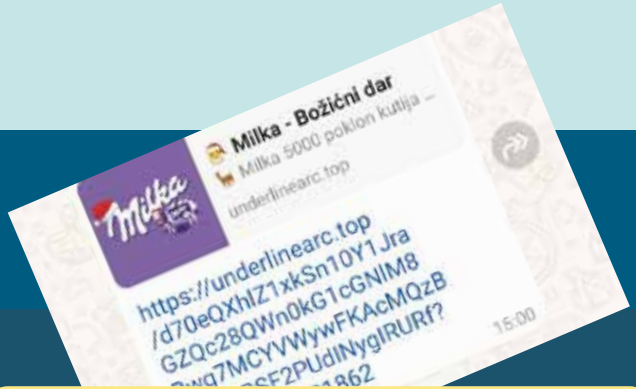
Što manje kolačića prihvatiš, manje ćeš podataka ostaviti u online svijetu.

Primijeni to pravilo na sve u životu ;)

Kolačići su mali digitalni tragovi koje internetske stranice ostavljaju na tvom uređaju kada ih posjetiš, kako bi zapamtile neke stvari o tebi i tvojim aktivnostima na internetu.

Vidjet ćeš sadržaj koji te stvarno zanima, oglasi će biti u skladu s tvojim interesima, nećeš morati iznova unositi svoje podatke kad se prijavljuješ, a oni analiziraju tvoje online navike te ograničavaju izlaganje neprimjerenim sadržajima.

Ako se pitaš zašto ti se na internetu prikazuju baš one stvari koje te zanimaju, odgovor je – upravo zahvaljujući kolačićima.



PROVJERI SVOJU ADRESU E-POŠTE NA HAVE I BEEN PWNED

Posjeti ovu mrežnu stranicu, unesi svoju adresu e-pošte i saznaj je li se ona pojavila u nekoj od hakiranih baza podataka.

Možeš se i pretplatiti kako bi na vrijeme saznao i na vrijeme reagirao, ako se to dogodi u budućnosti.

PAZI DA TE NE ULOVE

Phishing putem WhatsApp poruka je situacija u kojoj te netko pokušava prevariti da klikneš na lažnu poveznicu (link) kako bi ukrao tvoje podatke. Ako dobiješ poruku koja kaže “dobio si novi iPhone” ili nešto slično, a da zvuči predobro da bi bilo istinito, vjerojatno je u pitanju prijevara.

Nikad ne klikaj na sumnjive poveznice i ne dijeli svoje osobne podatke. Provjeri sumnjive poveznice putem stranice “Phishtank”, gdje već postoji velika baza poznatih phishing stranica. Sumnjive poveznice možeš upisati na Phishtank i provjeriti je li riječ o prevarantskoj stranici. Možeš prijaviti i bilo koju novu phishing stranicu na koju naiđeš, pomažući tako i drugima.

NEŠTO O DJEČJIM DIGITALNIM PRAVIMA…

Imaš pravo na edukaciju, na sudjelovanje, na odmor i igru, znati kako se prikupljaju tvoji osobni podaci, pravo biti siguran online… Znaš li tko te štiti na internetu??? Razmisli… Mama/tata? NE! Antivirusna zaštita? NE! I onda kad imaš roditeljsku zaštitu, budi svjestan da gotovo uvijek surfaš SAM i da si SAM odgovoran za sebe te da te antivirusna zaštita ne može dovoljno zaštititi!

OSVIJESTI NEVIDLJIVE TEHNOLOGIJE

Dok gledaš TikTok videa, kratke i opuštajuće sadržaje i slično, ne zaboravi da tvoju aktivnost prate nevidljivi mehanizmi koji prilagođavaju sadržaj koji gledaš tvojim interesima. Na taj način stvaraju se „mjehurići informacija“ pa imaš osjećaj da svi kupuju tvoje omiljeno sjajilo ili prate tvoj najdraži nogometni klub. Zamisli da na Wikipediji piše: svaka osoba će dobiti prilagođene definicije pojmova. Tada bi svatko mislio da je u pravu.

BUDI DIGITALNO EMPATIČAN!

Bilo da igraš igrice ili igrajući koristiš chat, objavljuješ fotografije s prijateljima (koji ti nisu dali za to dopuštenje) ili komentiraš tuđe objave - imaj na umu da tvoje riječi mogu izazvati loše osjećaje kod druge osobe. Često online govorimo i radimo stvari koje ne bi uživo. Zato pazi da tvoja digitalna osobnost ne bude loša verzija tvoje stvarne osobnosti! Ako nekoga neopravdano izbaciš iz WhatsApp grupe učinio si isto kao da si ga na školskom hodniku namjerno ignorirao.

Razlikuješ li slobodu govora od govora mržnje? Pokušaj što više razumjeti svoje emocije kako bi mogao razumjeti i tuđe.

Napravio si *meme* od nečije smiješne fotografije? Razmisli je li toj osobi ugodno i kako bi se ti osjećao na njenom mjestu.

Zapamti – svakim danom moramo biti sve svjesniji i odgovorniji kad su naši postupci u pitanju!

APLIKACIJA 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, a ističe koliko je važno pitati osobu s invaliditetom treba li pomoć prije nego što pomoć krenete pružati.

Ona pomaže da budete bolji i obzirniji prema osobama s invaliditetom u stvarnom svijetu i razumijete prepreke s kojima se suočavaju. Nadamo se da će vam pomoći da naučite kako biti odgovorniji i podržavajući građani.

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.

APLIKACIJA SUSRETNICA

Riješi se loših navika i pomozi drugima

Google efekt: navika prestanka pamćenja pojedinih informacija jer su uvijek dostupne putem tražilice

Vamping: ostajanje budnim cijelu noć kako bi gledali TV, surfali, igrali igre online…

Deepliking: grebanje po dalekoj prošlosti osobe koja nam se sviđa ili slučajno *lajkanje* fotografija objavljenih u prošlosti

Nomofobija: tjeskoba i nervoza zbog odvojenosti od pokretnog uređaja

Selfitis: *selfie* uvijek i svugdje

Ghosting: online ignoriranje drugoga, prestaju odgovori na pozive i poruke

Finsta: fake and Instagram, lažni profili na društvenim mrežama

Rinsta: real and Instargram, pravi profil za uži krug prijatelja na kojem se ne „glumi“ i pretvara da si nešto što nisi

No like fobija je strah koji ljudi osjećaju kada njihovi postovi na društvenim mrežama ne dobiju dovoljno lajkova

Cyber grooming čine odrasle osobe koje vas kontaktiraju na internetu i imaju loše namjere.

Doxxing ili **Outing** je otkrivanje osjetljivih ili osobnih podataka o nekome sa ciljem da ga se povrijedi ili ponizi.

Prijevara je slična outingu, ali razlikuje se po tome što se nasilnik sprijatelji sa svojom *žrtvom* i daje joj lažni osjećaj sigurnost, a žrtvu iskoristi te podijeli njezine tajne i privatne informacije s drugima.

Roasting ili Flaming uključuje oštre riječi i uvrede s namjerom da se druga osoba degradira i osjeća loše.

Catfishing tzv. catfish može stupiti u kontakt s tvojim vršnjakom koristeći lažni identitet, želi stvoriti povjerenje, ali zapravo će ga iskoristiti novčano i/ili emocionalno.

Happy slapping je napad grupe na pojedinca uz snimanje pokretnim uređajem i objavljivanje na internetu. Napad može predstavljati ismijavanje ili fizičko zlostavljanje.

Brain rot označava pogoršanje mentalnog stanja zbog pretjeranog gledanja trivijalnog sadržaja na internetu, poput beskonačnih videa na TikToku. *Oxford ju je proglasio riječju godine 2024. jer sve više ljudi brine kako internet utječe na naše misli i slobodno vrijeme.* U koliko termina si se prepoznao? Koliko situacija doživio?

Nisi preosjetljiv ako se loše osjećaš u gore opisanim situacijama. Ako ti nešto stvara nelagodu/sram/osjećaj krivnje zaista možeš sam to prekinuti. Nemoguće je danas koristiti digitalne tehnologije, a da se ponekad ne uhvatimo i u njihove zamke (čak su i Playstationu ukradeni podaci 7.7 mil korisnika). Zato je nužno što prije prijaviti takvo ponašanje (sjeti se samo digitalnih tragova, zahvaljujući njima nitko nije neuhvatljiv ☺!).

Znamo da nerado dijeliš sve informacije s roditeljima strahujući od kazne, ali baš tim dijeljenjem informacija i iskrenim razgovorom pokazao bi koliko si odgovoran i sposoban pomoći sebi i svima onima koji nemaju hrabrosti to nikome reći.

Screenshotaj poruke koje te vrijeđaju kako bi ih sačuvao za slučaj potrebe i zamisli sebe kao istražitelja koji skuplja dokaze kako bi uhvatio „krivca“.

Osim roditeljima, potpuno anonimno bilo koje opisano loše ponašanje drugih možeš prijaviti na:

APLIKACIJA RED BUTTON

APLIKACIJA TAKE IT DOWN

Imaš istražiteljsku narav? Web detektivi je program koji se fokusira na sigurnost djece i mladih na internetu, kao i na edukaciju o rizicima koji dolaze s korištenjem digitalnih platformi. Obučena djeca imaju čak i detektivsku iskaznicu!

APLIKACIJA WEB DETEKTIVI

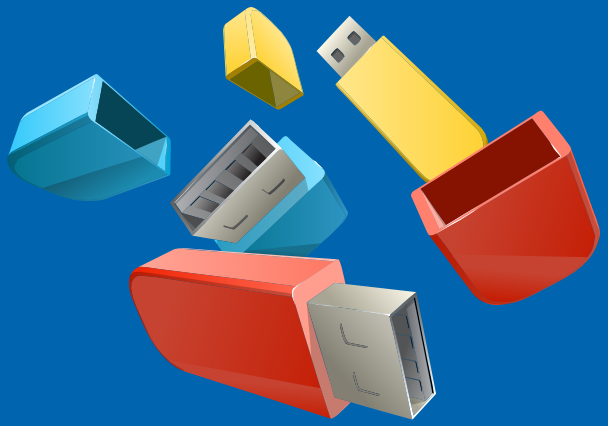
KLJUČEVI FINANCIJSKE SLOBODE

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 FaceID-om
2. **Ažuriranje:** redovito ažuriraj softver i 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:** kako smo naveli gore
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



NE BUDI PIRAT!

Jednostavna dostupnost tuđih autorskih djela (fotografije, crteži, video uradci, pisana djela), primjerice na internetu, ne znači da su ta djela slobodna za korištenje. Pravila koja vrijede u stvarnom svijetu (uzimanje tuđe majice zove se krađa) vrijede i za korištenja zaštićenih sadržaja objavljenih na internetu.

Neovlašteno korištenje autorskih djela predstavlja povredu prava, a zakonom je predviđena i kazna za takvo postupanje

NOVAC NE RASTE NA DRVETU

Stara dobra izreka kaže: Ako ne plaćaš proizvod, ti si proizvod!

Prati poruke koje ti šalje operator i uvijek o njima obavijesti svoje roditelje.
Budi oprezan i s porukama drugih pošiljatelja i nemoj automatski odgovarati na njih, pogotovo što u nekim porukama od tebe mogu tražiti i osobne podatke (adresu stanovanja, broj kartice roditelja).
Ne javljaj se na pozive s nepoznatog broja ni ne uzvraćaj nepoznate propuštene pozive, posebice ne na one koje nemaju oznaku +385 (jer moglo bi doći do neželjenog, većeg troška).
Kada putuješ u zemlju EU-a, nemaš problema jer surfaš i razgovaraš po cijeni kao doma – ROAM LIKE AT HOME. Ako te put odnese u npr. susjednu BIH, pazi jer moraš isključiti mobilne podatke kako ne bi došlo do neželjenog, većeg troška.
Slobodno skidaj aplikacije s AppStora/Google Play-a. Neke od njih su besplatne, međutim u njihovu korištenju mogu se pojaviti i neki dijelovi koji su naplatni (npr. igra *Dress to impress*, ako želiš druge zadiviti *outfitom* morat ćeš **to** dodatno platiti).
Zapamti: važno je uključiti “Provjere autentičnosti” kako bi spriječili neovlaštene kupnje.
Za povrat igara ili aplikacija imaš dva sata od trenutka kupnje (npr: otvori Google Play, idi na “Račun” i “Povijest narudžbi” kako bi zatražio povrat.) Maksimalni iznos za kupnju u Google Play-u je 49,77€, a ukupni mjesečni iznos je 66,36€. Možeš postaviti mjesečni proračun i “Roditeljski nadzor” kako bi ograničio korištenje.

KLJUČEVI OSOBNE SLOBODE

PRAVI KLJUČ U PRAVIM RUKAMA – TVOJE INFORMACIJE PRIPADAJU SAMO TEBI!

Ono što ne napraviš uvijek je važnije od onoga što si napravio

Kada smo kod nagovaranja, nemoj pristajati na snimanje, dijeljenje ili slanje vlastitih intimnih fotografija ili drugog neprimjerenog sadržaja ili videa pod nagovorom ili prisilom. Prijatelji koji te nagovaraju na takvo ponašanje nisu ti prijatelji, a odrasla osoba koja to od tebe traži te ne voli i nije dobronamjerna.

Opravdanje da svi to rade nije dovoljno i nećeš postati popularniji jer će se tvoja granica sve više pomicati. Reci odmah STOP svemu što ti stvara nelagodu.

Vjeruj svom osjećaju!

Dakle, razmisli 2 puta prije nego nešto objaviš, podijeliš ili proslijediš online.

Zapamti da tvoj digitalni trag ostaje, neovisno koliko god se ti mijenjao u životu.

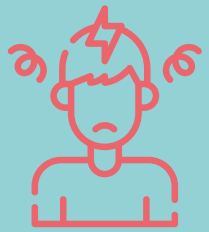
Zapitaj se bi li tebi to smetalo? Bi li takav sadržaj mogao pokazati svojim roditeljima?

Nagovaranje je zapravo nasilje. Zamisli samo kako b i ti bilo nelagodno kada bi se tvoje slike ili videa počeli dijeliti u školi. Zato budi oprezan jer je svijet interneta beskrajan, a objava prostog video uratka NIJE način povezivanja s vršnjacima. Ako netko ustraje predloži neku pozitivnu, tebi ugodnu aktivnost. U slučaju da druga strana na to ne pristane, jednostavno se udalji, jer vjeruj nam, to nije odnos koji želiš.

POPULARNOST NA KRATAK ROK, POSLJEDICE NA DUG – PROMISLI PRIJE OPASNOG IZAZOVA!

Ako gledaš TikTok izazove kad-tad ćeš naletjeti na neki kojeg ćeš poželjeti iskušati.

Nabrojat ćemo neke popularne i odmah te upozoriti na njihove opasnosti, za koje smo sigurni da si ih i sam svjestan. Ono što je jaaako bitno je da prije nego ih kreneš raditi, zastaneš, razmisliš i zapitaš se ima li šanse da nešto pri tome pođe po zlu? Udisanje cimeta, ležanje na cesti ili izazivanje opekotina ne čine se baš tako zabavno nakon malo promišljanja, zar ne? Budi kritičan kad su izazovi u pitanju jer nitko drugi to neće biti umjesto tebe. Promisli i o postupcima i porukama svog omiljenog youtubera, njemu je cilj zarada i popularnost.



KAD NARASTEM BIT ĆU INFLUENCER

Posao *influencera* može izgledati kao lagan put do popularnosti i bogatstva bez puno truda, učenja i discipline. Ipak, važno je znati da i uspjeh *influencera* zahtijeva mnogo rada, autentičnosti i odgovornosti, posebno prema mlađim pratiteljima. Mnogi *influenceri* kojima se divimo uložili su puno truda i vremena kako bi izgradili uspješnu karijeru.

Razmisli, reklamiraju li influenceri isključivo sadržaj koji vole?

Važno je i znati razlikovati pozitivan utjecaj od negativnog!

Primjer dobrog utjecaja *influencera*: Luka i Lea dijele savjete kako organiziraju vrijeme između škole, sporta i kreativnosti sa šminkom, potičući vas da se trudite u školi, bavite sportom i izrazite vlastitu kreativnost.

Primjer lošeg utjecaja *influencera*: Ivan i Petra, koji zanemaruju školu i promoviraju ljenčarenje ili pretjeranu šminku kao zamjenu za samopouzdanje, mogu stvoriti loše prioritete i nerealna očekivanja o ljepoti.

Utjecaj na druge znači odgovornost. Razmislite – kakav *influencer* želite biti?

ŠTO JE TO DSA (AKT O DIGITALNIM USLUGAMA)?

Svi bi se na internetu trebali osjećati sigurnima kada je u pitanju sadržaj ili ljudi, koji nas svojim postupcima i objavama mogu plašiti, ljutiti ili smetati. DSA je EU propis kojim se korisnicima, među kojima su i maloljetnici, omogućuje podnošenje prijava i pritužbi kada otkriju nezakonit ili drugi sadržaj koji ne bi trebao biti na internetu. Snapchat, Google, YouTube, Instagram i Facebook više ne dopuštaju oglašivačima prikazivanje ciljanih oglasa djeci.Na TikToku i YouTubeu računi djece, mlađe od 16 godina, sad automatski postaju privatni, pa takve videozapise mogu vidjeti samo njima poznati kontakti.

Zabranjuju se i „tamni obrasci", internetska sučelja (npr. Sheein) dizajnirana tako da nas navedu i zavaraju da učinimo stvari koje možda ne želimo učiniti, primjerice kupimo nešto što nam zapravo i ne treba. Mogu također utjecati na odluke ili nam otežati otkazivanje pretplate na usluge.

Zapamti da su brojne aplikacije stvarane tako da što više vremena provodiš na njima. Pobijedi sustav i ipak izađi na zrak - istraživanja kažu da se tvoja razina sreće smanjuje s vremenom provedenim online.

JA I UMJETNA INTELIGENCIJA

AI ili umjetna inteligencija postala je dio naše svakodnevice. Pomaže nam u učenju, pretraživanju i kreativnosti – možeš je koristiti za domaću zadaću, prevođenje, pa čak i za stvaranje umjetničkih djela. Na primjer, pokretnim uređajem možeš usmjeriti kameru na tekst i dobiti prijevod ili informacije o tome, što je super za školu. No, važno je zapamtiti da AI nije savršena i da ne smijemo sve što nam kaže uzimati zdravo za gotovo.

Kad razgovaraš s AI alatima, poput ChatGPT-a, razgovaraš sa strojem koji odgovore piše na temelju podataka koje su mu ljudi učinili dostupnim. Neki od tih podataka mogu biti netočni, pa je važno kritički razmišljati. Dok radiš zadaću, kombiniraj AI s provjerenim izvorima poput Pernica A1-linka, koji sadrži točne informacije za školu. AI može biti moćan alat, ali moraš ga koristiti s oprezom.

Na internetu često nailazimo na “botove”, što je skraćenica za “robot”. Oni pomažu u učenju, na primjer, Duolingo Bot za jezike ili Mathway Bot za matematiku. Ali pazi, neki botovi mogu biti zlonamjerni – koriste lažne slike ili dijele pogrešne informacije. Možeš ih provjeriti tako da profilne slike potražiš pomoću Google Image Searcha. Tako otkrivaš jesu li te slike stvarne ili stare i preuzete s interneta.

AI također donosi tehnologije poput deepfakea, koje mogu stvoriti lažne fotografije i videa. Ova tehnologija omogućuje da se tvoje lice “stavlja” u video ili u situacije u kojima nikad nisi bio. Zamisli video gdje se vidiš kako pušiš cigaru na krovu u Dubaiju, iako to nikada nisi napravio. Takve lažne sadržaje sve je teže prepoznati jer izgledaju uistinu stvarno.

Zato je važno da kritički razmišljaš o onomu što vidiš i dijeliš na internetu. Razgovaraj s roditeljima ili prijateljima o sadržajima koji ti se čine sumnjivima. AI je odličan pomoćnik, ali samo ako je koristiš odgovorno i s oprezom.

KUTAK ZA ODRASLE

Operatori elektroničkih usluga moraju omogućiti zabranu pristupa sadržajima neprikladnim za djecu. Tu opciju možete zatražiti prilikom sklapanja ugovora ili kasnije, a ostaje aktivna dok je sami ne ukinete.

Ako primite neprimjerene SMS ili MMS poruke, možete ih prijaviti svom operateru ili na e-mail nezeljeni.sms@hakom.hr, a brojevi s kojih dolaze bit će blokirani. Također, moguće je besplatno zatražiti zabranu primanja poruka s posebnom tarifom (npr. 6xx xxx, 8xx xxx).

Možete postaviti limit potrošnje (od 7 €) ili aktivirati roditeljsku zaštitu za TV, koja blokira neprimjerene sadržaje poput nasilnih ili pornografskih. Uz aplikacije poput Family Linka ili Dinner Timea, kontrolirajte vrijeme na uređajima, vrstu aplikacija i igrica.

Članak 95. stavak 4. Obiteljskog zakon propisuje:

Roditelji imaju pravo, dužnost i odgovornost nadzirati dijete u njegovu druženju s drugim osobama, kao i komunikaciju na društvenim mrežama, odnosno drugim oblicima elektroničke komunikacije te mu zabraniti druženja i komunikaciju koja nisu u skladu s djetetovom dobrobiti.

Zato dragi roditelji:

- ✓ Sudjelujte s djecom u izazovu: internet nije Baba Roga!
- ✓ Nakon izazova pročitajte brošuru
- ✓ Upoznajte se s kvizovima HAKOM-a
- ✓ Razmislite o roditeljskoj zaštiti
- ✓ Pogledajte stranice operatora na temu zaštite djece onlinе i uvjerite se koliko korisnih i kreativnih inicijativa operatori imaju
- ✓ Budite potpora svojoj djeci jer i mi odrasli smo često internet ovisnici
- ✓ Osvijestite informaciju da nekada dnevni razgovor roditelj – dijete traje samo 7 minuta ☺
- ✓ Za sva korisnička pitanja, slobodno posjetite www.hakom.hr
- ✓ Pogledajte s djecom QRkod Luke Bulića pjesme i youtube kanala sa filmićem zaštita djece
- ✓ Edukacija je prvi korak, a u virtualnom svijetu ona je cjeloživotna. Zato učimo i budimo potpora našoj djeci!

Koliko god digitalne vještine danas bile na cijeni, one ne vrijede ništa bez životnih vještina koje omogućavaju rješavanje problema i zato je važno da ih kao roditelji damo svojoj djeci.

KAKO ZAŠTITITI DJECU NA INTERNETU?

MALIŠANI PODUČAVAJU LUKU BULIĆA O SIGURNOM INTERNETU

IZAZOV: INTERNET NIJE BABA ROGA!

Dragi svi, preostao nam je jedan zadatak za kraj.

Ponesite brošuru kući i s roditeljima prođite sljedeća pitanja i zadatke.

1

Imaju li tvoji roditelji na društvenim mrežama kao prijatelje/pratitelje nepoznate osobe? Ukoliko imaju reci im da si ti svoje radi sigurnosti izbrisao i objasni im zašto to trebaju i oni učiniti.

2

Pohvali se roditeljima da si na www.howsecureismypassword.net potvrdio kako imaš izvrsnu, jaku lozinku. Neka i oni provjere/promijene svoju, a objasni im i kako je ispravno koristiti.

3

Nemojte samo vi biti ispitivani, otvorite Kalkulator privatnosti i prođite s roditeljima pitanja (razina težine je od lagane do teške) pa im dajte ocjenu na kraju „testa“. Budite strogi, ali pravedni.

4

Osim gorućeg Eiffelovog tornja, pokažite roditeljima još par deepfake videa i/ili fotografija te im objasnite što taj termin znači (neka i oni budu informirani kao i vi).

5

5. Imaju li tvoji roditelji TikTok? Pogledajte TikTok izazove navedene u brošuri i/ili im pojasni u čemu se sastoje i zašto su opasni?

6

6. Pokaži roditeljima par videa koji si objavio na TikToku i neki snap… Sad shvaćaš da objavljuješ samo ono što mogu vidjeti i brižne oči tvojih roditelja ☺.

U školi komentirajte međusobno kako je prošlo i na kojem pitanju je bio najveći GLAM(BLAM) jer najbolje učimo jedni od drugih.

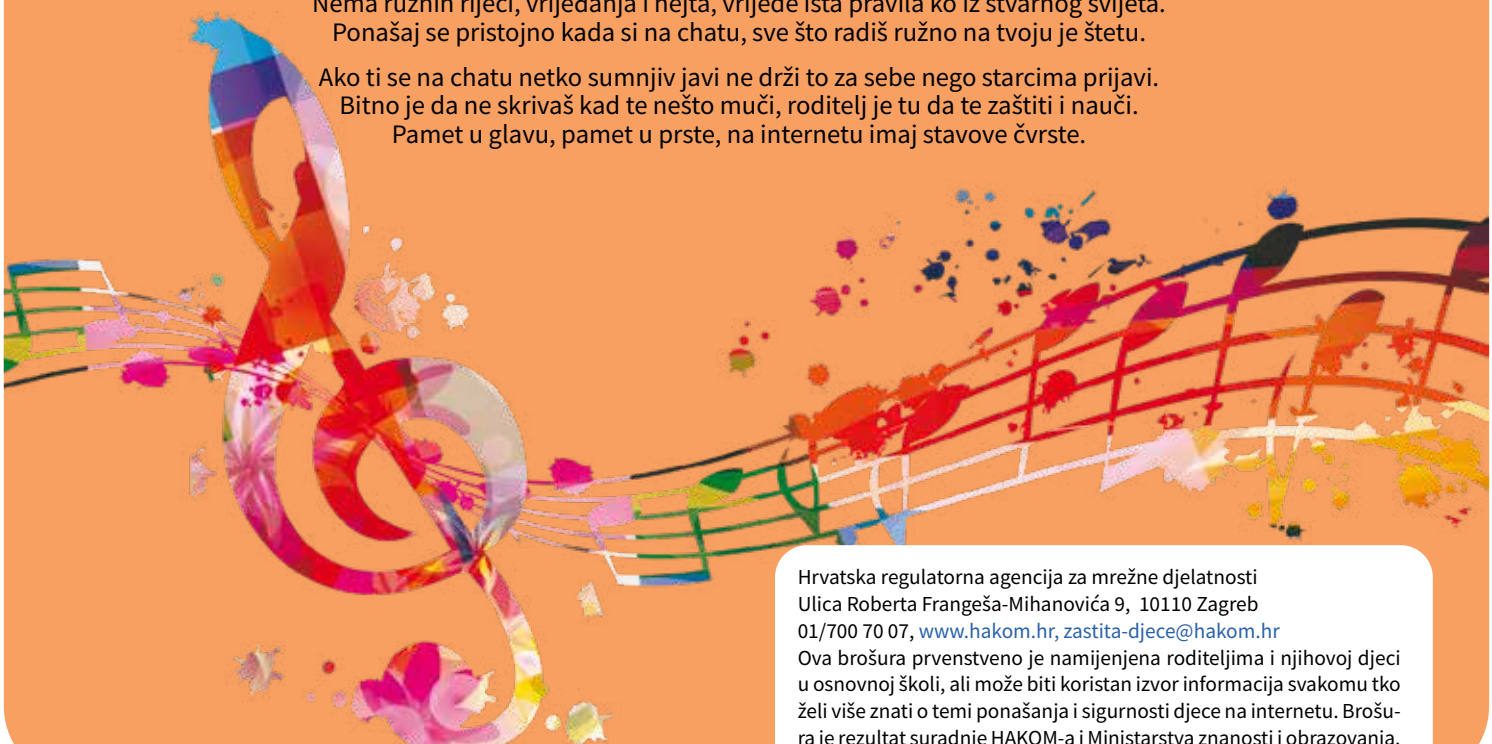
Pamet u glavu, pamet u prste, na internetu imaj stavove čvrste.

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 i obrazovanja.
Godina proizvodnje: 2025.