



Be cyber smart!

Kako zaštititi decu na internetu — vodič za roditelje



Razgovarajte o bezbednosti na internetu na vreme i budite proaktivan roditelj

Internet je neverovatno sredstvo za učenje, druženje i zabavu dece. Međutim, s obzirom na to da je svaki treći korisnik interneta mlađi od 18 godina, rizici povezani s onlajn aktivnostima su značajni i nastavljaju da rastu. Otprilike troje od četvero dece širom sveta iskusilo je bar jedan cyber rizik.¹ Kako biste zaštitili svoju decu, ovaj vodič za internet bezbednost pruža dragocene savete i preporuke. Kao roditelj ili staratelj, zaštita onlajn sigurnosti vašeg deteta danas je važnija nego ikad.

¹ The Child onlajn Safety Index, DQ Institute, 2022.

Počnite da razgovarate sa decom o bezbednosti na internetu u ranom uzrastu. Vođenjem ovih razgovora od malih nogu, možete im pomoći da donose pametne odluke i razviju zdrave navike u onlajn svetu. Edukovanje o odgovornom korišćenju interneta, zaštiti privatnosti i potencijalnim opasnostima takođe će ih zaštititi od rizika. Zapamtite, nikada nije prerano da postavite temelje za sigurno korišćenje interneta.

- **Mladi su uvek željni da uče.** Naučite ih kako da kreiraju sigurne lozinke, prepoznaju bezbedne veb stranice, izbegavaju prevare, praktikuju odgovorno ponašanje na internetu i usvoje druge veštine za sigurnu onlajn aktivnost.
- **Ne delite lične podatke.** Podsetite decu da nikada ne dele lične informacije, poput punog imena, kućne adrese, lozinke ili broja telefona sa osobama koje ne poznaju.

- **Budite oprezni sa nepoznatim osobama.** Razgovarajte sa decom o mogućim opasnostima komunikacije sa nepoznatim ljudima na internetu i objasnite im da nikada ne treba da se sastaju uživo sa osobama koje su upoznali onlajn bez vašeg znanja i saglasnosti.
- **Postavljajte pitanja.** Obavezno postavljajte svom detetu pitanja o njihovim onlajn aktivnostima - koje sajtove posećuju i s kim komuniciraju. Ohrabrite ga da iskreno razgovara o tome šta prati, gleda i deli na internetu.
- **Postavite jasna pravila.** Kontrolišite vreme provedeno pred ekranom tako što ćete definisati koliko dugo dete može da bude onlajn i šta može da radi. Vreme provedeno ispred ekrana koje nije vezano za školu može biti dostupno nakon što završe domaći zadatak ili tokom vikenda. Računare i druge uređaje držite u zajedničkim prostorijama kako biste nadgledali sve aktivnosti..
- **Ograničite pristup internetu i pratite aktivnosti.** Ne morate da budete stručnjak za sajber bezbednost da biste zaštitili svoju decu na internetu. Aplikacije za roditeljsku kontrolu i opcije ugrađene u uređaje i Wi-Fi rutere su jednostavne za korišćenje. One vam omogućavaju da podesite vreme pristupa internetu, pratite aktivnosti i blokirate određene kategorije sajtova. Znanje o tome šta vaša deca rade na internetu može pomoći u njihovoj zaštiti. Iskoristite ovu priliku da pokažete svojoj deci koji su sajtovi prikladni za njihovu uzrasnu grupu
- **Budite dobar primer.** Postavite dobar primer svojim prisustvom na mreži. Demonstrirajte sigurno ponašanje i prakse.

Onlajn igrice? Igrajte pametno!

Onlajn igre mogu biti zabavna društvena aktivnost, ali takođe nose određene rizike. Sajber nasilje, onlajn predatori i skriveni troškovi su neki od problema kojih bi roditelji trebalo da budu svesni. Da biste osigurali sigurnost svoje dece, evo nekoliko saveta koje možete pratiti:

- Koristite dostupne roditeljske kontrole kako biste sprečili preuzimanje neprimerenih aplikacija i igara.
- Postavite lozinke kako biste sprečili kupovine unutar igre.
- Ustanovite jasna očekivanja i pravila o vremenskim ograničenjima i vrstama igara koje su dozvoljene.
- Ograničite dopisivanje u okviru igre na razgovore koji su povezani sa samom igrom.
- Uverite se da vaše dete razume važnost čuvanja ličnih informacija privatnim i da ih nikada ne deli onlajn.
- Recite im da odmah prijave odrasloj osobi bilo kakvo nasilje.

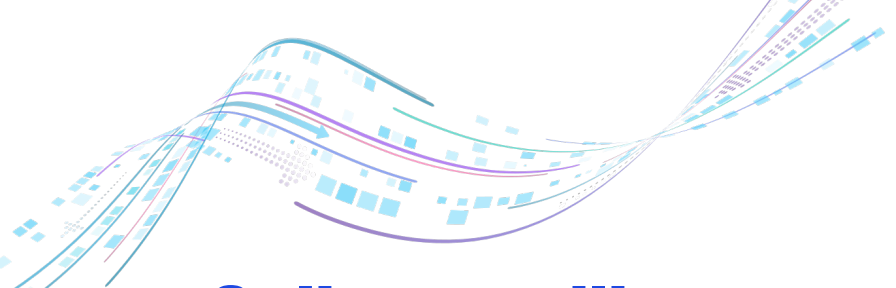
Bezbednost na društvenim mrežama

Društvene mreže su postale sastavni deo naših svakodnevnih života i dragoceni alati za komunikaciju i zabavu. Međutim, postoje i značajni rizici povezani s ovim platformama, posebno za decu. Ukoliko deca neodgovorno koriste društvene mreže, to ih može izložiti raznim opasnostima, uključujući sajber nasilje i onlajn predatore. Da biste zaštitili svoju decu, evo nekoliko saveta koje treba imati na umu:

- **Starosna ograničenja.** Većina društvenih mreža ima ograničenja prema uzrastu. Vodite računa da se ta pravila poštuju i pratite njihovo korišćenje.
- **Razmislite pre objavljivanja.** Naučite svoju decu da budu svesna komentara i slika koje objavljuju i naglasite im da nikada ne dele lične informacije kao što su njihova starost, škola, adresa ili puno ime. Objasnite im da, jednom kada nešto postane onlajn, ostaje na internetu. Ovo je posebno važno kako deca odrastu i počinju da traže prve letnje poslove, jer poslodavci često proveravaju prisustvo kandidata na internetu.

- **Pratite svoje dete.** Nadgledajte aktivnosti na društvenim mrežama tako što ćete pratiti svoje dete onlajn. Ne morate učestvovati, samo redovno pregledajte profile i objave.
- **Pregledajte stranice za roditeljsku podršku na društvenim mrežama.** Da biste saznali više o zaštiti naloga vašeg deteta na društvenim mrežama, pregledajte stranice za podršku roditeljima. Osigurajte da je profil vašeg deteta uvek podešen na „privatni“ režim putem podešavanja naloga i naučite ih o postavkama privatnosti.





Sajber nasilje

Sajber nasilje je vrsta nasilja koja se odvija putem elektronskih sredstava komunikacije i nažalost je postalo veoma rasprostranjeno. Iako ima sličnosti sa tradicionalnim nasiljem, sajber nasilje može naneti još veću štetu jer napadač može nastaviti da uznemirava žrtvu bez obzira na to gde se ona nalazi. Sa internetom i mobilnim telefonima, svako može postati sajber nasilnik u bilo kojem trenutku i sa bilo koje lokacije. Evo kako možete pomoći:



Pričajte sa decom

Važno je danas razgovarati s decom o sajber nasilju. Potičite otvorenu komunikaciju kako bi se osećali prijatno da vam prijave takve situacije. Edukujte ih da:

- Odmah prijavite uvredljive ili bolne komentare, bez obzira na to da li su oni meta ili ne.
- Budite oprezni sa onim što govore, šalju, objavljuju ili bloguju o drugima — nenamerna povreda je takođe nasilje.



Prepoznajte

Znakovi da je neko žrtva sajber nasilja:

- Pokazivanje iznenadne ljutnje, depresije ili frustracije nakon korišćenja bilo kog uređaja ili izbegavanje korišćenja uređaja uopšte.
- Nelagodnost oko odlaska u školu ili učestvovanja u grupnim ili timskim aktivnostima.
- Neuobičajeno se povlači od prijatelja i članova porodice.



Reagujte

Roditelji i deca treba da preduzmu akciju na sledeće načine:

- Čuvanje uvredljivih poruka, objava i e-mailova.
- Ne odgovarati na njih i ne brisati ih.
- Prijavljivanje ID-ja onlajn i blokiranje korisnika kako bi se sprečila dalja interakcija.
- Prijavljivanje problema školi vašeg deteta ili policiji, ako je to potrebno.

Bezbedno prijavljivanje i odjavljivanje

Upravljanje velikim brojem lozinki može biti izazov, naročito za decu koja ih teško pamte. Međutim, važno je razumeti da su lozinke osnovna zaštita od moguće zloupotrebe ličnih podataka, koja može ugroziti njihovu bezbednost kako na internetu, tako i van mreže. Da biste obezbedili bezbedno prijavljivanje i odjavljivanje, evo nekoliko ključnih saveta koji će pomoći deci da bolje zaštite svoje lične informacije:

Pažljivo birajte korisnička imena

- Izbegavajte korišćenje punog imena, starosti, adrese, datuma rođenja, pola ili drugih ličnih informacija.
- Savetujte deci da se konsultuju s odraslom osobom prilikom kreiranja korisničkih imena ako imaju nedoumica.

Vežbajte sigurnost lozinki:

- Pokažite deci kako da kombinuju fraze, brojeve, simbole i velika i mala slova.
- Naglasite im da nikada ne ponavljaju ili ponovo koriste lozinke i da nikada ne dele lozinku ili je ne daju ako ih neko zatraži.
- Izbegavajte lozinke koje se lako pogađaju, poput datuma rođenja ili omiljenog sporta ili aktivnosti.

- Pokušajte da koristite menadžer lozinki i savetujte svojoj deci da zapamte samo tri lozinke: jednu za školu, jednu za svoj računar i jednu za menadžer lozinki — dok će sve ostale lozinke biti pohranjene tamo.
- Podstičite ih da koriste dvostruku autentifikaciju gde god je to moguće.

Zaštita vaših ličnih podataka

Podsetite svoje dete da se uvek odjavi kada napusti sajt ili platformu.

Izbegavajte besplatan WI-FI i rizik od krađe podataka od strane hakera.

Nikada ne delite svoje pristupne podatke s drugima, uključujući prijatelje.

Savetujte deci da nikada ne daju lične informacije kao što su puno ime, kućna adresa ili broj telefona osobama koje ne poznaju.

Kada posećujete veb sajtove na telefonima, ne unosite korisnička imena i lozinke.



Bezbedno i odgovorno korišćenje veštačke inteligencije

Kako alati zasnovani na veštačkoj inteligenciji (AI) postaju sve popularniji, prirodno je da i deca pokazuju interesovanje za njih. Zato je važno razgovarati sa njima o odgovornom i prikladnom korišćenju tehnologije. Sledeći saveti mogu da pomognu vašoj porodici da zajedno istražujete i učite o veštačkoj inteligenciji.

Kako to funkcioniše? Objasnite svojoj deci kako funkcioniše AI, kako bi mogla da cene njene prednosti, razumeju potencijalna ograničenja i nauče kako da je efikasno koriste. Dajte im nekoliko primera s kojima su možda već upoznati kako biste im pomogli da shvate o čemu se radi.

Kako je koristiti? AI alati mogu pomoći deci da budu kreativna i nauče nove veštine. Razgovarajte sa njima o tehnologijama i alatima koji ih zanimaju. Pomozite im da razmisle na koje načine im ovi alati mogu pomoći u učenju i ličnom razvoju. Podstičite ih da budu kritični prema informacijama koje dobijaju iz nove tehnologije i da koriste svoju kreativnost kako bi dopunili veštačku inteligenciju.

Koji su rizici? Deca treba da razumeju da veštačka inteligencija ima ograničenja koja mogu dovesti do netačnih i pristrasnih rezultata. Hakeri takođe mogu manipulirati veštačkom inteligencijom menjajući podatke, što može dovesti do pogrešnih predikcija. Ne zaboravite da podsetite decu da veštačka inteligencija nema emocionalno razumevanje i ne može zameniti ljudske odnose i povezanosti.

Kako bezbedno koristiti veštačku inteligenciju?

- **Budite svesni ličnih informacija.**

Deca ne bi trebalo da dele osetljive informacije, kao što su puno ime i prezime, adresa, broj telefona ili finansijski podaci, osim ako koriste pouzdanu platformu i razumeju na koji način se upravlja ličnim podacima.

- **Razumevanje podešavanja privatnosti.**

Odvojite vreme da pregledate i prilagodite postavke privatnosti na AI platformama u skladu sa podešavanjima koja vam odgovaraju.

- **Ne preterujte s deljenjem.**

Ograničite količinu ličnih informacija koje su javno dostupne i obratite pažnju na to koje se informacije prikupljaju.

- **Razmišljajte kritički.**

Zapamtite da AI sistemi nisu savršeni i mogu praviti greške. Zamolite decu da proveravaju činjenice, upoređuju informacije i razmatraju različite perspektive pre nego što donesu zaključke ili odluke isključivo na osnovu rezultata koje generiše AI.

- **Prijavite neprikladan sadržaj.**

Ako vaše dete naiđe na uvredljiv ili štetan sadržaj ili doživi neprimerenu interakciju, naučite ih da to prijave platformi, pružaocu usluga ili odrasloj osobi kojoj veruju.

- **Budite oprezni sa porukama koje generiše AI.**

Ako prime neočekivane ili sumnjive poruke sa AI naloga ili čet botova, neka ne dele lične informacije niti se upuštaju u razgovore koji ih čine nelagodnim.

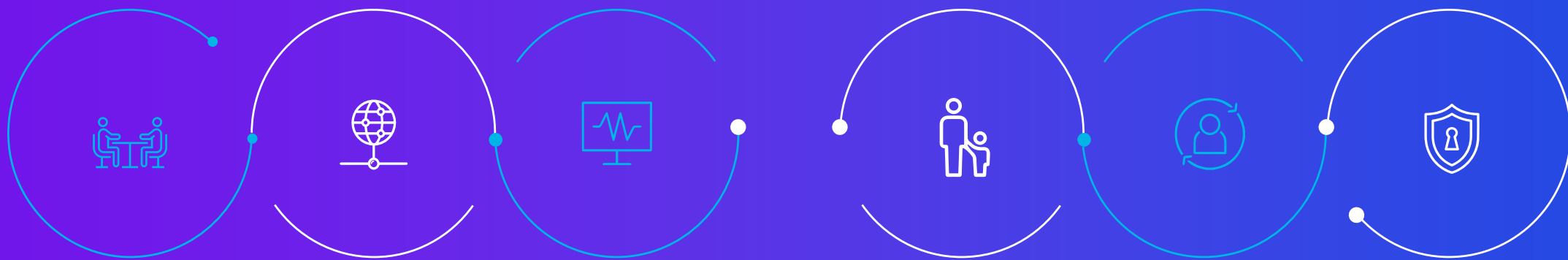
- **Ne oslanjajte se isključivo na AI.** Izbegavajte prekomerno oslanjanje na veštačku inteligenciju za

donošenje odluka. Objasnite im da korišćenje AI za školski rad koji nisu sami kreirali može biti smatrano plagiranjem ili prevareom. Umesto toga, upoznajte ih sa obrazovnim AI alatima koji dopunjuju njihovo učenje.

- **Budite informisani.**

Pratite najnovija dostignuća i promene u oblasti veštačke inteligencije kako biste bolje razumeli njene mogućnosti, ograničenja i potencijalne rizike. Ovo znanje će omogućiti vašoj porodici da donosi dobro informisane odluke i odgovorno koristi veštačku inteligenciju.

Šest koraka za bezbednije onlajn okruženje za vašu decu



01

Budite uključeni svaki dan.

Redovno razgovarajte sa decom o značaju bezbednosti na internetu. Pre nego što primenite bilo kakve mere zaštite, razgovarajte sa svojom decom zašto planirate da to uradite, kako bi se osećala poštovano u vezi s njihovom privatnošću.

02

Roditeljska kontrola.

Razmotrite korišćenje alata za roditeljsku kontrolu kako biste upravljali sve većim brojem uređaja koje vaša deca koriste i kako biste ih zaštitili na internetu. Ovi alati mogu pomoći tako što blokiraju nepoželjni veb sadržaj, ograničavaju korišćenje rizičnih aplikacija i još mnogo toga. Važno je naučiti kako ih koristiti i redovno ih ažurirati.

03

Podesite bezbednosne opcije.

Bez obzira na uređaj, aplikaciju ili servis koji vaše dete koristi, važno je da pravilno podesite bezbednosne opcije kako biste obezbedili sigurnije okruženje.

Koristite sajtove poput: internetmatters.org za korak-po-korak podešavanje bezbednosnih opcija.

Obratite pažnju na privatnost profila, filtriranje neprimerenog sadržaja, komunikaciju sa nepoznatim osobama i deljenje lokacije kako biste dodatno zaštitili svoje dete na internetu.

04

Roditeljske kontrole.

Razmotrite korišćenje roditeljskih kontrola za ograničavanje vremena pred ekranom, blokiranje aplikacija i praćenje aktivnosti. Ove alate je potrebno podesiti i redovno ažurirati. Upoznajte se i sa njihovim ograničenjima, odnosno aplikacijama koje ne mogu da kontrolišu. Oni ne mogu da zamene korake 1–3. Otvoreno razgovarajte sa detetom o praćenju aktivnosti.

05

Pratite i prilagođavajte

Redovno preispitujte navike korišćenja tehnologije u porodici. Tehnologija može stvoriti osećaj zavisnosti čak i kod odraslih, zato, ako nešto ne funkcioniše, preispitajte situaciju, razgovarajte i prilagodite pristup.

Kako dete odrasta, razmotrite koje zaštitne mere možete postepeno ublažiti.

06

Osnove sajber bezbednosti.

Ne zaboravite na zaštitu od svakodnevnih internet pretnji:

- Instalirajte antivirusni softver.
- Koristite duže lozinke koje se lako pamte, a teško pogađaju. Razmotrite korišćenje menadžera lozinki.
- Redovno pravite rezervne kopije važnih podataka.
- Vodite računa o digitalnom tragu svoje porodice.
- Pokažite deci primere fišing poruka i internet prevara kako bi ih lakše prepoznali.

Dodatne informacije i resursi

Kako biste pomogli deci i tinejdžerima da razviju bezbedne navike na internetu, važno je da promovirate odgovorno ponašanje na mreži i ostanete uključeni u njihove digitalne aktivnosti. Za više informacija i saveta o bezbednom korišćenju interneta posetite kpmg.com/cyberday.





kpmg.com



Informacije sadržane u ovom dokumentu su opšte prirode i nisu namenjene okolnostima određenog pojedinca ili pravnog lica. Iako nastojimo da pružimo tačne i pravovremene informacije, ne možemo garantovati da su te informacije tačne onda kada su primljene niti da će ostati tačne u budućnosti. Ne bi trebalo postupati na osnovu takvih informacija bez prethodnog odgovarajućeg stručnog saveta datog nakon detaljnog ispitivanja određene situacije.

KPMG International Limited je privatno englesko društvo ograničeno garancijom. KPMG International Limited i njegova povezana pravna lica ne pružaju usluge klijentima. Za više informacija o našoj strukturi posetite kpmg.com/governance.

© 2026 KPMG d.o.o. Beograd, srpsko društvo s ograničenom odgovornošću i firma članica KPMG globalne organizacije nezavisnih firmi članica povezanih sa KPMG International Limited, privatnim engleskim društvom ograničenim garancijom. Sva prava zaštićena.

KPMG ime i logo su zaštitni znaci koje nezavisne firme članice KPMG globalne organizacije koriste u skladu sa licencom.