

VODIČ ZA RODITELJE

Enkriptovane aplikacije

Koje aplikacije za dopisivanje zaista čuvaju privatnost vašeg djeteta, i koje su prave za koji uzrast.

@isoc.me
www.internetsociety.me

PRIJE NEGO ŠTO POČNETE

Kome pripada ključ?

Gotovo svaka aplikacija tvrdi da je „bezbjedna“ ili „enkriptovana“. Ovaj vodič vam pomaže da provjerite ono najvažnije: **da li poruke vašeg djeteta može da pročita samo osoba kojoj su namijenjene, ili i kompanija koja pruža uslugu.**

Bez enkripcije

● Nije zaštićeno

KO MOŽE DA PROČITA

Svako ko presretne poruku na putu

Kao razglednica: vidi je svako kroz čije ruke prođe

Enkripcija u prenosu

● Djelimično

KO MOŽE DA PROČITA

Kompanija koja pruža uslugu i svako ko dođe do njenih servera

Kao pismo u zaključanom kombiju: na putu je zaštićeno, ali se u pošti otvara

Enkripcija s kraja na kraj

● Zaštićeno

KO MOŽE DA PROČITA

Samo pošiljalac i primalac

Kao kutija čiji ključ imaju samo dvije osobe: ni pošta je ne može otvoriti

Kako da čitate ocjene

● Zaštićeno

Privatne poruke i grupe enkriptovane su s kraja na kraj automatski, bez ikakvog podešavanja.

● Djelimično

Neki razgovori su zaštićeni, drugi nisu, ili zaštitu morate sami uključiti.

● Nije zaštićeno

Kompanija može da pročita sadržaj poruka, osim ako ne koristite posebnu opciju.

Stanje: oktobar 2026. Aplikacije mijenjaju pravila — Instagram je, na primjer, u maju 2026. potpuno ukinuo enkripciju s kraja na kraj u porukama. Provjeravajte vodič barem jednom godišnje.

PREGLED

Poređenje aplikacija

Kolona „Šta nije zaštićeno“ pokazuje gdje i u „zelenim“ aplikacijama treba obratiti pažnju.

Aplikacija	Poruke jedan na jedan	Grupe	Šta nije zaštićeno	Ocjena
Signal	Automatski	Automatski	—	 Zaštićeno
WhatsApp	Automatski	Automatski	Rezervne kopije (dok ih sami ne zaštitite), kanali	 Zaštićeno
Viber	Automatski	Automatski	Zajednice (Communities), kanali, četovi sa botovima	 Zaštićeno
iMessage (iPhone)	Automatski	Automatski	Rezervne kopije na iCloudu (osim uz Naprednu zaštitu podataka)	 Zaštićeno
Messenger	Automatski	Morate uključiti	Grupe bez uključene zaštite	 Djelimično
Google Messages	Automatski, između korisnika RCS-a	Automatski, između korisnika RCS-a	Obični SMS i MMS; razgovori sa iPhone-om tek se uvode	 Djelimično
Snapchat	Fotografije i video („snapovi“)	Ne	Tekstualne poruke i grupe	 Djelimično
Telegram	Samo u „tajnim četovima“	Ne	Svi obični četovi, grupe i kanali	 Nije zaštićeno
Discord	Ne (pozivi i video jesu)	Ne	Sve tekstualne poruke	 Nije zaštićeno
Instagram	Ne (ukinuto u maju 2026.)	Ne	Sve poruke	 Nije zaštićeno
TikTok	Ne	Ne	Sve poruke	 Nije zaštićeno
Obični SMS	Ne	Ne	Sve poruke	 Nije zaštićeno

DETALJI

Šta treba da znate o pojedinim aplikacijama

Signal

● Zaštićeno

Napravljen isključivo oko enkripcije s kraja na kraj i prikuplja vrlo malo podataka. Manje je popularan među djecom, pa je najkorisniji ako ga koristi cijela porodica.

WhatsApp

● Zaštićeno

Automatski šifruje sve privatne poruke, grupe i pozive. Slaba tačka su rezervne kopije na Google Drive-u ili iCloudu: nijesu šifrovane s kraja na kraj dok ne uključite tu opciju (Četovi → Rezervna kopija četova → Šifrovana rezervna kopija).

Viber

● Zaštićeno

Veoma popularan u Crnoj Gori. Automatski šifruje privatne i grupne četove i pozive. Zajednice, kanali i četovi sa botovima zaštićeni su samo u prenosu, jer njihov sadržaj vide i novi članovi.

iMessage

● Zaštićeno

Poruke između Apple uređaja automatski su šifrovane s kraja na kraj. Rezervne kopije na iCloudu dobijaju istu zaštitu tek kada uključite Naprednu zaštitu podataka.

Messenger

● Djelimično

Od kraja 2023. automatski šifruje razgovore jedan na jedan, ali za grupne četove zaštitu i dalje morate posebno uključiti.

Google Messages

● Djelimično

Šifruje RCS poruke između korisnika koji imaju RCS, dok obični SMS nije zaštićen. Apple je u maju 2026. počeo probno da uvodi šifrovane RCS poruke između iPhone-a i Android telefona, pa će se zaštita postepeno širiti.

Snapchat

● Djelimično

Šifruje fotografije i video snimke poslate jednoj osobi, ali tekstualne poruke i grupni četovi nijesu u potpunosti zaštićeni na isti način. Javne priče (Stories) nikada nisu privatne.

Telegram

● Nije zaštićeno

Često se pogrešno smatra potpuno šifrovanim. Obični četovi čuvaju se na Telegramovim serverima; enkripcija s kraja na kraj postoji samo u „tajnim četovima“ koje morate sami pokrenuti, i to samo za razgovor dvije osobe. Grupe i kanali nikada nisu šifrovani s kraja na kraj, a velike javne grupe olakšavaju kontakt sa nepoznatima.

Discord

● Nije zaštićeno

Od 2026. šifruje s kraja na kraj glasovne i video pozive, ali tekstualne poruke nijesu zaštićene na taj način.

Instagram

● Nije zaštićeno

Ukinuo je 8. maja 2026. opcionu enkripciju s kraja na kraj u porukama, pa kompanija Meta sada može da pristupi sadržaju svih poruka.

TikTok

● Nije zaštićeno

Ne nudi enkripciju s kraja na kraj u porukama i najavio je da je neće uvesti, navodeći bezbjednost mladih kao razlog.

Obični SMS

● Nije zaštićeno

Obične SMS i MMS poruke nijesu šifrovane. Za privatne razgovore izaberite neku od „zelenih“ aplikacija.

Kako da provjerite sami: otvorite razgovor i potražite oznaku katanca ili poruku „zaštićeno enkripcijom s kraja na kraj“ na vrhu četa. Ako je nema, pretpostavite da kompanija može da pročita poruke.

PREPORUKE

Šta odgovara kojem uzrastu

Većina aplikacija za dopisivanje zahtijeva da korisnik ima najmanje 13 godina. Kada dijete koristi aplikaciju prije propisanog uzrasta, ne dobija zaštite namijenjene maloljetnicima, jer ga aplikacija smatra starijim nego što jeste. Zato su preporuke za mlađu djecu usmjerene na porodične naloge kojima upravljaju roditelji.

0-8 GODINA

- Dijete ne treba da ima sopstvene aplikacije za dopisivanje.
- Za kontakt sa bakom, djedom ili rođacima koristite porodični čet na **vašem** telefonu, u „zelenoj“ aplikaciji, uz vaše prisustvo.
- Ovo je pravi uzrast za prve razgovore o tome šta je privatno i zašto se ne razgovara sa nepoznatima.

9-12 GODINA

- Ako dijete dobije telefon, birajte opcije predviđene za djecu: **dječji Apple nalog** uz Porodično dijeljenje (iMessage) ili **dječji Google nalog** uz Family Link (Google Messages).
- Dijete neka se dopisuje samo sa kontaktima koje i vi poznajete.
- Izbjegavajte aplikacije sa javnim grupama i serverima, gdje se lako dolazi u kontakt sa nepoznatim odraslima (npr. Telegram, Discord), kao i društvene mreže čije poruke nisu zaštićene.
- Razgovarajte o enkripciji: „Ono što napišeš drugarici vidi samo ona — zato je važno kome pišeš.“

13–15

GODINA

- Dogovorite jednu glavnu aplikaciju za privatno dopisivanje, sa „zelenom“ ocjenom.
- Zajedno podesite: ko može da dijete doda u grupe (samo kontakti), ko može da ga kontaktira i da li se vidi kada je bilo na mreži.
- Objasnite razliku: poruke na Instagramu, TikTok i u Snapchat četovi može da pročita kompanija, i to su mjesta na kojima nepoznati najčešće prvi put pišu djeci. Ako neko nepoznat traži da „pređu na drugu aplikaciju“, to je znak upozorenja.
- Pokažite kako se prijavljuje i blokira u svakoj aplikaciji koju dijete koristi.

16–18

GODINA

- Tinejdžer sve više samostalno odlučuje — vaša uloga je savjetnička.
- Naučite ga da uključi šifrovane rezervne kopije, nestajuće poruke kada mu odgovaraju i zaključavanje aplikacije PIN-om.
- Objasnite kako da prepozna kada razgovor nije šifrovan (npr. obični Telegram čet) i zašto osjetljive stvari — fotografije, zdravstvena pitanja, lične dokumente — ne treba slati tim putem.
- Razgovarajte otvoreno o ucjeni intimnim fotografijama: enkripcija štiti poruku na putu, ali ne i od osobe kojoj je poslata.

Savjet: preporuke važe za uzrast, ali svako dijete je drugačije. Važnije od godina je da li dijete razumije sa kim razgovara i da li zna da vam se obrati kada nešto nije u redu.

ZA JEDNO SA DJETETOM

Podešavanja koja vrijedi uključiti

Prođite ovu listu na svakom uređaju koji dijete koristi i označite šta ste uradili.

- ☐ **Šifrovana rezervna kopija** u WhatsApp-u (Četovi → Rezervna kopija četova).
- ☐ **Napredna zaštita podataka** na iCloudu za iPhone, da i rezervne kopije poruka budu šifrovane s kraja na kraj.
- ☐ **Ko može da me doda u grupe:** samo moji kontakti (WhatsApp, Viber, Telegram).
- ☐ **Zaključavanje telefona** PIN-om, otiskom prsta ili licem.
- ☐ **Zaključavanje aplikacije** ili skrivanje četova, ako dijete dijeli uređaj sa drugima.
- ☐ **Provjera enkripcije u čet:** oznaka katanca ili poruka „zaštićeno enkripcijom s kraja na kraj“ na vrhu razgovora.
- ☐ **Prijava i blokiranje:** dijete zna gdje se nalaze u svakoj aplikaciji koju koristi.

Enkripcija nije sve

Enkripcija štiti poruku od onih koji ne bi trebalo da je vide. Ona ne štiti dijete od osobe sa kojom se dopisuje. Zato su najvažnije tri stvari i dalje iste: znati sa kim dijete razgovara, naučiti ga da prepozna manipulaciju i pritisak, i izgraditi povjerenje da vam se obrati kada nešto nije u redu — bez straha od kazne.

**Ključ privatnih razgovora
vašeg djeteta treba da
ostane u vašim rukama.**