Organization for Security and Co-operation in Europe
Mission to Bosnia and Herzegovina

WOMEN 4CYBER
EUROPEAN CYBER SECURITY ORGANISATION

SIGURNO KORIŠTENJE ALATA UMJETNE INTELIGENCIJE (AI)

KRATKI VODIČ ZA GRAĐANSTVO



Disclaimer

The preparation of this document was supported by the OSCE Mission to BiH. Any point of view, statement or opinion expressed in this document, if not explicitly indicated as coming from the OSCE Mission to BiH, does not necessarily reflect the official policy of the OSCE Mission to BiH.

Šta je umjetna inteligencija ?

Umjetna inteligencija, ili AI, naziv je za tehnologije i sisteme koji pokazuju inteligentno ponašanje analizirajući dostupne podatke i poduzimajući određene radnje – uz određeni stepen autonomije, te koje mogu generisati sadržaj i izvršavati zadatke koji su nekada bili mogući samo uz ljudski rad i inteligenciju, poput kreiranja teksta, prepoznavanja govora, sažimanja informacija, prevođenja ili izrade raznih planova i projekata.

Umjetna inteligencija (AI) jeste veliko postignuće ubrzanog tehnološkog razvoja i efektivan alat na raspolaganju ljudima u današnjem svijetu.

U svakodnevici, AI može biti korisna za izradu nacrta mnogih tekstova, obrade tema, objašnjenja pojmova u bilo kojoj oblasti, usporedbu proizvoda, prevođenje, te može dati ideje za planiranje putovanja, uređenja, poslovnih koraka i procesa u mnogim sferama života i rada .

Kako pametno i sigurno koristiti AI

AI nam pomaže u analizi informacija, generisanju ideja i podršci odlučivanju, te konstantno koristi metode učenja za postizanje optimalnih rezultata. Međutim, AI ne razumije situacije na isti način kao čovjek, nema etičko rasuđivanje i odgovornost. Zbog toga ne može zamijeniti logičnost ljudske procjene, ljudsko iskustvo i donošenje odluka.

Pošto AI ne razumije informacije kao ljudi, te može proizvesti netačne, nepotpune ili obmanjujuće rezultate. AI odgovore uvijek treba kritički procijeniti i provjeriti, naročito kada je riječ o osjetljivijim temama, kao što su **zdravlje, finansije, posao, pravna pitanja, sigurnost, ljudska prava ili porodica/djeca.**



Glavni rizici

Generalno, razmatranja i razne analize vezano za korištenja AI alata, izdvajaju nekoliko ponavljajućih rizika:

- AI može generisati netačne informacije i predstaviti ih kao činjenice, može prenijeti ili pojačati pristrasnosti;
- može biti zloupotrijebljena za kreiranje uvjerljivih prevara, lažnih sadržaja i manipulativnih poruka.
- Rizik nastaje i kada korisnici u AI alate unose lične, osjetljive ili povjerljive podatke, koji mogu biti pohranjeni ili obrađivani na način koji korisnik ne očekuje.

Dodatno, na društvenim mrežama i online platformama, problem nije samo što se sadržaj može lako proizvesti, već u tome što algoritmi često favorizuju sadržaj koji privlači i zadržava pažnju i angažman, a to nije nužno sadržaj koji je najtačniji, najkorisniji ili najpouzdaniji.

U BiH jezičkom i društvenom prostoru potreban je dodatni oprez: AI može pogrešno protumačiti **nijanse jezika, humor, ironiju, mržnju ili istorijski kontekst.** To znači da nešto što AI označi kao “neutralno”, “normalno” ili “sigurno” u stvarnosti može biti netačno, štetno, diskriminatorno ili manipulativno.

Praktični savjeti za sigurniju upotrebu

Kada koristite AI, postavite sebi tri pitanja:

Da li AI navodi izvor informacije?

Da li je informacija još uvijek tačna i aktuelna?

Kako mogu provjeriti njenu tačnost i pouzdanost?

Ovo je posebno važno kad postoji mogućost da informacije mogu uticati na vaše zdravlje, finansije, privatnost, reputaciju ili sigurnost. Profesionalnije napisana poruka ne smije vas odvratiti od provjere sadržaja i konteksta.

PREPORUKA KAKO RADITI	PREPORUKA ŠTA NE RADITI
Koristite AI za ideje, nacrte, objašnjenja i sažimanje informacija	Ne prepuštajte AI-ju konačnu odluku o važnoj temi
Tražite izvor i datum odgovora	Ne vjerujte prvom odgovoru samo zato što zvuči uvjerljivo ili profesionalno
Koristite opšte i anonimne primjere kada postavljate pitanja AI-ju	Ne unosite lične, zdravstvene, finansijske i ostale povjerljive podatke
Ako AI preporuči web stranicu ili link provjerite domen, pošiljaoca i kontekst	Ne otvarajte odmah linkove iz hitnih ili neočekivanih poruka
Preuzimajte aplikacije i datoteke samo iz službenih i provjerenih izvora	Ne instalirajte aplikaciju ili dodatak samo zato što ga je AI preporučio
Budite transparentni ako je AI pomogao pri pisanju ili obradi sadržaja	Ne predstavljaj sadržaj koji je nastao uz pomoć AI-a kao vlastiti rad
Upozorite druge ako primijetite novu vrstu prevare ili obmane	Ne zadržavajte informaciju za sebe ako može pomoći i drugima da prepoznaju ili izbjegnu prevaru

Privatnost i lični podaci

Najvažnije pravilo je: **u javne AI alate ne unosite ono što ne biste objavili javno ili poslali nepoznatoj osobi.**

To uključuje puno ime i prezime, adresu, broj telefona, e-mail, JMBG ili drugi identifikacijski broj, bankovne podatke, zdravstvene podatke, podatke o djeci, kao i tuđe podatke.

Jednako je važno zaštititi i poslovne informacije. U javne AI alate ne bi trebalo unositi interne dokumente, zapisnike sa sastanaka, e-mailove, ugovore, pravne informacije. izvorni kod, poslovne strategije, tabele s podacima kupaca, zaposlenika ili partnera, kao ni dokumente koji “iz konteksta” mogu otkriti o kojoj se osobi ili organizaciji radi. Čak i kada obrišete ime, osoba ponekad ostaje prepoznatljiva kroz datum, lokaciju, opis događaja ili kombinaciju detalja.

Ako baš morate opisati stvarni slučaj AI-u, koristite opšte i neprepoznatljive opise. Umjesto stvarnih imena i detalja koristite izraze poput **“osoba A”, “kolega”, “zaposlenik” ili “korisnik”,** i uklonite sve nepotrebne identifikatore.

Prije korištenja AI alata provjerite njegove postavke privatnosti, istoriju razgovora i postoji li opcija u postavkama da se vaši podaci ne koriste za poboljšanje modela.

Važno je prepoznati AI prevare i deepfake (digitalni falsifikat) sadržaje

Generativna AI je prevarantima olakšala kreiranje poruka, fotografija, glasovnih snimaka i videa koji djeluju uvjerljivo. Danas je moguće relativno jednostavno napraviti sadržaj koji izgleda ili zvuči kao da dolazi od osobe kojoj vjerujete.

Budite posebno oprezni ako dobijete poziv ili glasovnu poruku u kojoj neko zvuči kao član porodice, prijatelj ili nadređena osoba i hitno traži uplatu ili slanje podataka ili neku drugu neuobičajenu radnju.

Najvažniji znakovi za uzbunu su i dalje isti: poruka je **neočekivana,** traži **hitnu reakciju,** pokušava izazvati **strah, sažaljenje ili paniku,** traži **novac, lozinku, pristup računu ili dokumente,** i želi da djelujete **odmah i bez provjere.**

Danas bolja gramatika, profesionalniji dizajn ili uvjerljiv glas ne čine poruku automatski sigurnom; zapitajte se ima li poruka smisla, jeste li je očekivali i pokušava li utjecati na vašu odluku.

Ako primite glasovnu poruku ili neočekivan poziv, **ne uzvraćajte na broj ili link iz poruke** i ne djelujte odmah. Nazovite osobu ili instituciju na poznat vam broj, ili ih kontaktirajte drugim, odvojenim kanalom. Ako video, fotografija ili audio djeluju “uvjerljivo”, to je razlog za dodatnu provjeru, a ne za bržu reakciju.

Na poslu poštujte interna pravila i ne prebacujte poslovne podatke u javno dostupne servise bez dozvole i procjene, te koristite samo odobrene alate i račune.

Ako AI predloži da preuzmete aplikaciju, igru, dodatak, knjigu ili datoteku, najprije provjerite postoji li to stvarno i preuzmite samo iz službene trgovine ili od provjerenog proizvođača. **Ne instalirajte ništa “naslijepo” samo zato što je to AI predložila.**

Djeca i AI

Djeca sve češće koriste AI za školu, pretragu informacija i zabavu, pa je važno da pravila budu jednostavna i jasna. UNICEF preporučuje da roditelji i skrbnici s djecom **zajedno istražuju AI,** razgovaraju o odgovorima koje alat daje, objašnjavaju što AI može, a što ne može, štite privatnost djeteta i razvijaju kritičko mišljenje kroz provjeru odgovora i izvora.

Dijete treba znati da AI može pomoći pri učenju, ali ne treba postati prečica umjesto razmišljanja. UNICEF izričito savjetuje da se AI koristi kao koristan alat, a ne kao zamjena za vlastito razmišljanje, te da roditelji zajedno s djecom pregledaju što alat prikuplja i dijeli.

Za djecu i mlade dodatno vrijedi pravilo da AI ne zamjenjuje prijatelje, roditelje, učitelje ni stručnu pomoć.

Roditelji, ne branite korištenje AI djeci apriori, nego učite zajedno i postavite granice.

Šta učiniti ako ste oštećeni

Ako sumnjate da ste nasjeli na AI-podržanu prevaru ili ste unijeli podatke na lažnu stranicu, prvo **prekinite komunikaciju.** Zatim **promijenite lozinke,** posebno na računima koji su povezani s e-mailom, bankarstvom ili društvenim mrežama. Za bankovne podatke, odmah **kontaktirajte banku.**

Sačuvajte dokaze: snimke ekrana, poruke, broj s kojeg je poziv došao, linkove i vrijeme incidenta. Ako smatrate da je počinjeno krivično djelo ili druga nelegalna radnja, **prijavite slučaj** policiji ili relevantnoj službi. Na kraju, **upozorite druge.** Znanje o prevarama treba dijeliti s porodicom, kolegama i prijateljima, jer se ista kampanja prevare obično šalje velikom broju ljudi.

Brza samoprovjera

Prije nego što nešto unesem u AI

- ☐ Znam koji alat koristim i za šta ga koristim.
- ☐ Provjerio/la sam postavke privatnosti i istoriju razgovora.
- ☐ Ne unosim lične, zdravstvene, finansijske ni povjerljive poslovne podatke.
- ☐ Ako opisujem stvarni slučaj, anonimizirao/la sam ga.

Prije nego što povjerujem odgovoru

- ☐ Provjerio/la sam datum i izvor.
- ☐ Usporedio/la sam odgovor s barem još jednim pouzdanim izvorom.
- ☐ Zapitao/la sam se: ima li ovo smisla u stvarnom kontekstu?
- ☐ Znam da profesionalan ton ne znači da je odgovor tačan.

Prije nego što kliknem, preuzmem ili pošaljem

- ☐ Provjerio/la sam domenu i pošiljatelja.
- ☐ Ne klikam na hitne i neočekivane poruke bez provjere.
- ☐ Ako AI preporuči alat ili aplikaciju, prvo provjerim službeni izvor.
- ☐ Uređaji i aplikacije su mi ažurirani.

Ako poruka traži novac, lozinku ili dokumente

- ☐ Zastajem i ne reagujem odmah.
- ☐ Potvrđujem zahtjev drugim kanalom.
- ☐ Ne vjerujem samo videu, glasovnoj poruci ili fotografiji.
- ☐ Ako sumnjam na prevaru, ne nastavljam komunikaciju.

Ako mislim da sam oštećen/a

- ☐ Mijenjam lozinke.
- ☐ Ako su ugroženi bankovni podaci, zovem banku.
- ☐ Čuvam dokaze.
- ☐ Prijavljujem policiji i službama.
- ☐ Upozoravam druge oko sebe.

Kratki podsjetnik

Mogu li vjerovati AI odgovoru ako zvuči sigurno i stručno?

Ne vjerovati potpuno i automatski. AI može dati uvjerljiv, a netačan odgovor, pa uvijek moram provjeriti izvor, datum i kontekst.

Smijem li u AI kopirati ugovor, službeni e-mail ili tabelu sa podacima?

Ne u javni alat, osim ako je to izričito odobreno, procijenjeno i zaštićeno. To posebno vrijedi za lične i povjerljive podatke.

Kako da prepoznam AI prevaru?

Gledam znakove hitnosti, pritiska, traženja novca ili lozinki, neočekivanog kontakta i poruka koje me žele spriječiti da provjerim informaciju drugim kanalom

Smiju li djeca koristiti AI sama?

Djeca mogu koristiti uz jasna pravila, razgovor i nadzor primjeren dobi. Najvažniji su privatnost, provjera odgovora i razumijevanje da AI nije zamjena za vlastito razmišljanje

Trebam li reći da sam koristio/la AI za pripremu projekata?

Da, posebno u školi, na poslu, u javnim objavama, prezentacijama, prevodima i istraživačkom radu. Transparentnost povećava povjerenje.

