Kako koristiti ChatGPT na siguran način?

SMJERNICE ZA SIGURNO I ODGOVORNO KORIŠTENJE AI MODELA

Sve što unesemo u ChatGPT se pohranjuje i koristi za njegovo daljnje 'treniranje' (bilo to uneseno u obliku teksta, u obliku prijenosa datoteke ili davanja povratnih informacija).

Podaci korisnika ChatGPT-a mogu biti dijeljeni s trećim stranama (uz pristanak ili u posebnim okolnostima). AI sustavi su trenutno 'crna kutija' za običnog korisnika, ne znamo na koji način se naši podaci obrađuju i spremaju te koriste li se primjerene mjere za zaštitu cjelovitosti, povjerljivosti i dostupnosti podataka.

Budući da se u kratkom periodu dogodilo nekoliko sigurnosnih incidenata, savjetujemo pridržavanje sljedećih pravila:

1_ Prije korištenja ChatGPT-a (ili drugih AI modela) savjetujte se sa svojim nadređenim.

2_ Provjerite URL na kojem se nalazite prilikom korištenja ChatGPT-a, kako ne bi unijeli podatke u zlonamjernu stranicu koja imitira sustav.

3_ Ne unosite osobne, osjetljive ili povjerljive podatke u ChatGPT.

4_ Redovito brišite razgovore unutar sustava koji vam više ne trebaju.

5_ Ne koristite poslovni račun za prijavu u ChatGPT.

6_ Podatke koje vam sustav generira dvostruko provjerite.

Ne znamo otkud se podaci vuku, a sustav zna samouvjereno iznositi netočne podatke. Sustav može razviti pristranost, ali i namjerno biti konfiguriran na taj način. Dobiveni sadržaj je izveden iz sadržaja koji su prethodno generirali drugi i stoga je potrebno obratiti pažnju da se ne radi o sadržaju koji je zaštićen autorskim ili srodnim pravim. Također, ako generirani sadržaj sadrži osobne podatke isti ne treba koristiti jer postoji velika vjerojatnost da podaci nisu prikupljeni u svrhu za koja je potrebna nama te bi takvo korištenje predstavljalo kršenje pozitivnih propisa kojima se uređuju osobni podaci.

7_ Poštujte sigurnosnu politiku CARNET-a i propisana pravila za zaštitu i povjerljivost podataka.

8_ S posebnim oprezom koristite dodatke za preglednike (add-on/plug-in) koji omogućuju pristup ChatGPT-u, jer su već iskorišteni za krađu podataka.

9_ Ne unosite dijelove kôda u ChatGPT.

10_ Redovito ažurirajte svoje sustave.

11_ Redovito se informirajte i educirajte o novim prijetnjama te mjerama zaštite.

Za najnovije informacije o najboljim praksama u korištenju umjetne inteligencije, pratite objave Nacionalnog CERT-a.

cert.hr/tag/ai/
facebook.com/CERT.hr
twitter.com/HRCERT