**DI žaidimų meškos paslauga arba lengviau asmeninių duomenų neišviliosi**

Pastarosiomis savaitėmis visame pasaulyje žaibiškai plintanti pramoga pasitelkiant dirbtinį intelektą (DI) susikurti savo virtualų herojų ar lėlę (angl. AI doll) nėra toks jau nekaltas žaidimas. Kad sukurtų norimą rezultatą, DI technologijos prašo pasidalinti savo nuotraukomis, taip pat nurodyti asmeninių duomenų. Kur jūsų duomenys nukeliauja toliau ir kas juos naudoja? Tai keli iš klausimų, apie kuriuos siūlo pagalvoti IT saugumo ekspertai.

**Pataria saugoti šią informaciją**

Į dirbtinio intelekto įrankį įkeliate norimą savo nuotrauką, nurodote, kaip norite būti pavaizduotas, kas jums patinka kasdieniame gyvenime ir *voila* –  už kelių sekundžių matote, kaip atrodo į dėžutę supakuota jūsų lėlė antrininkė. Smagu ir linksma, bet ar sutiktumėte dirbtiniam intelektui atiduoti valdyti savo „Instagram“ ar „Facebook“ paskyrų duomenis? Rezultatas, kaip ir naudojant dirbtinį intelektą pramogoms, toks pats – savanoriškai dalinamės asmenine informacija. Kieno serveriuose ši informacija galiausiai nugula? Ar internetinė erdvė kada nors ją pašalins? Anot duomenų apsaugos įrankius kuriančios įmonės „Surfshark“ informacinių technologijų saugumo vadovo Tomo Stamulio, atsakymas yra „Ne“ arba „Negalime to žinoti“.

„Tačiau tikrai įmanoma, kad informacija, pagal kurią esame lengvai identifikuojami, ateityje bus panaudota prieš mus. Duomenys gali būti nutekinami ir naudojami priešiškai, pavyzdžiui, sukčiaujant ar siekiant prisijungti prie žmogaus asmeninių paskyrų“, – įspėja T. Stamulis.

„Surfshark“ ekspertas primena, kokios informacijos apie save negalima atskleisti dirbtinio intelekto šaltiniams, įskaitant žaidimus ir pramogas. Tai asmens kodas, pilnas vardas ir pavardė, telefono numeris. Prie jautrių ir nedalintinų duomenų priskiriama ir informacija apie vaikus, nepilnamečius giminaičius ar draugus, banko ar finansinių paslaugų teikėjo pavadinimai. Taip pat patariama nesidalinti klinikiniais ar medicininiais duomenimis, atskleidžiant informaciją apie sveikatos sutrikimus, ligas, mat, nutekinimo atveju, tai gali padaryti ekonominės žalos, pavyzdžiui, siekiant įsidarbinti. Galiausiai su mažai patikimais šaltiniais nepatariama dalintis asmeninėmis nuotraukomis ar vaizdo įrašais, kadangi vaizdinė informacija gali būti panaudota klastojant žmogaus pirštų antspaudus ir kitus biometrinius duomenis.

**3 žaidimo taisyklės**

Paklaustas, ar vertėtų neįsitraukti į greitai plintančias, madingas DI pramogas, „Surfshark“ ekspertas teigia, kad svarbiausia yra žinoti, kaip apsaugoti save dirbtinio intelekto ir interneto erdvėse ir pateikia 3 esmines taisykles, kurių verta laikytis.

„Pirma, įsitikinkite, kad jūsų paskyra, su kuria dalyvaujate DI žaidimuose, yra stipri ir saugi. Tai reiškia, jog tiek kompiuteryje, tiek telefone turite įdiegtą VPN apsaugą naršymui, paskyra yra apsaugota stipriu slaptažodžiu ir su įjungta 2 faktorių autentifikacija“, – atkreipia dėmesį T. Stamulis.

Antra, jungdamiesi prie dirbtinio intelekto žaidimų, pateikite kiek įmanoma mažiau tikrų duomenų apie save ir gyvenamąją vietą. Galiausiai, jei naudojatės DI pramogų programėlėmis, atminkite, kad yra įmanoma, jog jūsų duomenys bus nutekinti. Dėl šios priežasties patartina naudotis tokiais DI įrankiais, kurie nerenka jūsų naršymo istorijos, geriausiai prie DI įrankių jungtis nematomu (*incognito*) režimu ir ne su pagrindinio savo el. pašto paskyra, o jei yra galimybė, naudotis neprisijungus.

**Kaip skaityti privatumo politiką?**

Kibernetinio saugumo ekspertai įsitikinę, kad dešimties puslapių ilgio privatumo politikas skaito tikrai retas. O visgi, norint naudotis dirbtiniu intelektu saugiai, derėtų susirasti ir peržvelgti bent jau esminius punktus. Kokie jie?

* Ieškokite sąrašo, paaiškinančio, kokie jūsų asmens duomenys bus renkami, pavyzdžiui, vardas, el. paštas, kompiuterio IP adresas.
* Įsitikinkite, ar nerenkami jautrūs asmeniniai duomenys, tokie kaip jūsų lokacija, biometriniai duomenys, informacija apie finansus ar sveikatą.
* Privatumo politika turi nurodyti, kokiu tikslu naudos jūsų duomenis. Pavyzdžiui, teikti ir tobulinti paslaugas, bendrinti su trečiosiomis šalimis, rinkodaros ar kitais konkrečiais tikslais. Žvelkite įtariai, jei privatumo politikoje įrašytos neaiškios frazės, tokios kaip „naudojama verslo tikslais“ arba „paslaugoms gerinti“.
* Peržiūrėkite, su kuo bus dalinamasi jūsų duomenimis. Patikimi šaltiniai gana konkrečiai nurodo trečiąsias šalis ar jų kategorijas, kurioms perduodami duomenys. Abejotino patikimumo šaltiniai apsiriboja abstrakčiomis frazėmis – „informacija dalijamasi su „patikimais partneriais“.
* Patikrinkite, ar duomenimis bus dalinamasi tarptautiniu mastu, ypač su šalimis, garsėjančiomis žema asmens duomenų apsauga.
* Žinokite, kaip ilgai programėlė ar svetainė saugos jūsų duomenis. Venkite naudotis paslaugomis, įvardijančiomis, kad „duomenis saugos neribotą laiką, nebent ištrinsite anketą“.

**Apie „Surfshark**“

„Surfshark“ yra 2018 m. Lietuvoje įkurta tarptautinė kibernetinio saugumo bendrovė, vystanti produktus „Surfshark VPN“, „Surfshark Antivirus“, „Alternative ID“ (el. pašto ir asmeninės informacijos maskavimo įrankį), „Surfshark Alert“ (skirtą duomenų nutekėjimui aptikti) bei „Incogni“ (asmeninių duomenų pašalinimo paslaugą). 2022 m. „Surfshark“ kartu su „Nord Security“ paskelbti antruoju oficialiu vienaragiu Lietuvoje. Šiemet „Surfshark“ antrą kartą pateko į prestižinį [„Financial Times“ 1000 greičiausiai augančių Europos įmonių reitingą.](https://www.ft.com/ft1000-2024)