COLUMN

De nieuwste hype: ChatGPT

(Of: “Gaat dit ons helpen of leveren we weer een stukje privacy in?”)

Heeft u dat ook wel eens dat u zich afvraagt “Wat moet ik hier nu van vinden?”. Mij overkwam dat kortgeleden toen er een stortvloed van berichten over ChatGPT, u weet wel dat nieuwe linguïstische AI taalmodel, over ons uitgestort werd.
Omdat ik duidelijk niet bij de early adapters behoor heb ik het de eerste tijd maar even over me heen laten komen. Echter de toenemend enthousiaste (en mogelijk opgeklopte) verhalen hebben me verleid om hier toch eens mee te gaan experimenteren.
U begrijpt het waarschijnlijk al……., leest u nu mijn column of die van een kunstmatige intelligentie?

Natuurlijk heb ik het geprobeerd! Alleen bleek ChatGPT niet in staat om een column naar mijn stijl te schrijven. Ondanks dat ik hem naar mijn website met alle gepubliceerde columns heb verwezen kreeg ik als reactie dat hij onvoldoende informatie had om in mijn stijl een column te schrijven.
Als alternatief kreeg ik een column voorgeschoteld zoals een opiniemaker die zou kunnen schrijven en helaas bleek ongeveer vijfhonderd woorden ook teveel van het goede, hij bleef steken halverwege het 330ste woord. Inhoudelijk was het wel goed te lezen, dus daar gaan we meer van horen.

Nu ik toch zelf deze column moet schrijven, en me dus echt in het onderwerp moet verdiepen, heb ik eens over het business model nagedacht. Het formele business model van OpenAI (de eigenaar van ChatGPT) is erg idealistisch omschreven, maar omdat o.a. Microsoft er nu 10 mil-jard dollar in gaat investeren neemt mijn huiver over veiligheid en privacy wel toe.

Ik denk dat met de komst van een AI chat programma mensen verleid gaan worden veel, en steeds intiemere, vragen te stellen. Een beetje slimme AI robot slaat dit natuurlijk op en zal dit ongetwijfeld via een achterdeurtje wel willen verkopen. Omdat je bij het registreren voor een login account naast je mail adres ook jouw (mobiele) telefoonnummer op moet geven is e.e.a. makkelijk naar de persoon te herleiden en liggen al jouw vragen, wensen en onzekerheden open en bloot voor het oprapen.

Natuurlijk heb ik ChatGPT gevraagd of OpenAI te vertrouwen is en daar geeft het een mooi poli-tiek nietszeggend antwoord op.
Op de vraag wie de aandeelhouders van OpenAI zijn wil het om formele redenen geen antwoord geven en daarvan word ik dan weer ongerust. Wat valt er te verbergen? Deze info is toch op Internet te vinden en dit zou toch de bron van de kennis van ChatGPT zijn?

Dan maar even een uitstapje naar Google, hier kom ik, naast Microsoft, o.a. op Infosys, Khosla Ventures en Reid Hoffman uit.
Op de vraag of ze ooit in een privacy schandaal betrokken zijn geweest geeft ChatGPT dat Microsoft en Infosys beiden 3x betrapt zijn op het schenden van de privacy regels. In dit geval de weinig beperkende Amerikaanse regels, dus dat belooft wat voor de toekomst.

Ga ik ChatGPT in de toekomst nog gebruiken? Ik denk van wel, maar ik ben me er zeer bewust van dat ik niet elke vraag kan stellen. Je weet maar nooit hoe dit nog eens tegen je gebruikt gaat worden.

Mijn conclusie, eigenlijk een mooie ontwikkeling die wel veel zorgen baart over de privacy en veiligheid, maar waarschijnlijk net zo verslavend (voor sommigen) zal zijn als Facebook, Instagram TikTok en andere (on)sociale media.

Jan W. Veltman

Reageren?
jan.w.veltman@technology2success.nl