url: <https://botcore.ai/blog/6-ways-to-enhance-chatbot-security/>

veel speculatie en vragen over chatbot security

* Hoe veilig zijn ze
* Waar is informatie opgeslaan
* Hoe data beschermd wordt
* Welke kanalen het toegang tot heeft
* …

2 soorten security bezorgdheden

* Bedreigingen
  + Malware
  + DDoS attacks
  + Hackers proberen systeem plat te leggen of data stelen
* Kwetsbaarheden
  + Dat is als een systeem open is voor een aanval 🡪 kwetsbaar
  + Slecht geprogrammeerd
  + Slechte beveiliging
  + …

Manieren om chatbots veiliger te maken

* End-to-end encryptie
  + Berichten encrypteren die over het kanaal gaan, enkel zender en ontvanger kunnen het lezen
  + Als hackers de data hebben, zijn ze er niets mee door dat het geëncrypteerd is
* Two-factor auth
  + Gebruikers moeten hun identiteit bevestigen door 2 verschillende kanalen
* User identity authentication
  + Login credentials
  + Meest gebruikt
  + Enkel bij login kan je chatbot gebruiken
* Voldoen aan GDPR
* Channel autorisatie
* Authentication timeouts
  + Na verloop van tijd verloop je chatsessie en moet je opnieuw authenticeren
* Biometric authentication
  + Vingerafdruk, oog, gezichtsherkenning
* Self destructing messages
  + Als gebruikers gevoelige informatie als accountgegevens of dergelijke moeten doorgeven kan je je afvragen waar die informatie opgeslaan wordt
    - Oplossing: self d messages waarbij de berichten na verloop van tijd voor eeuwig worden vernietigd en niet worden bijgehouden