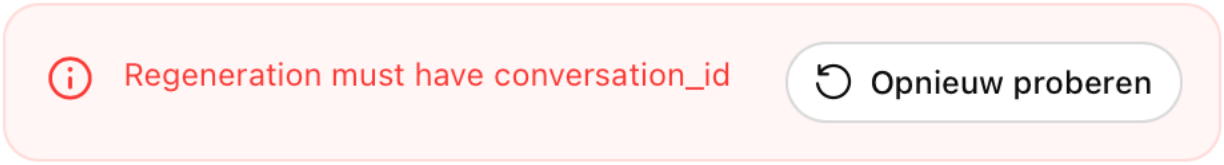
DIGITAAL FORENSISCH RAPPORT bij Digitale stalkende Criminelen betaalde ChatGPT

REGELMATIGE MELDING IN MIJN BETAALDE CHATGPT:



1. Is sabotage van ChatGPT technisch mogelijk?

Ja, maar alleen **indirect**, via de volgende aanvalsvectoren:

- **Wifi / netwerkmanipulatie**
  Een aanvaller die toegang heeft tot mijn router of wifi-netwerk kan verkeer manipuleren (man-in-the-middle aanval). Daarmee kan hij sessies verstoren of mijn verbinding instabiel maken.
- **Gestolen Apple-ID of Mac-inloggegevens**
  Als mijn Apple-ID is gecompromitteerd, kan een aanvaller wachtwoorden synchroniseren, inloggen in mijn iCloud-sleutelhanger, en dus ook bij mijn OpenAI/ChatGPT-account komen. Daarmee kan hij sessies kapen of mijn account tijdelijk buitensluiten.
- **Cookie-/sessie-kapingen**
  Hackers die via malware of browser-exploits mijn sessie-cookies buitmaken, kunnen in mijn ChatGPT-account terechtkomen zonder wachtwoord. Dat sluit aan bij wat ik in mijn rapport beschrijf: langdurige toegang via gestolen sessietokens.
- **Koppeling met andere accounts**
  Omdat ook mijn WordPress, LinkedIn en Xing zijn misbruikt, is het plausibel dat dezelfde indringer ook probeert mijn ChatGPT-account te misbruiken. Betaalde accounts zijn interessant omdat ze gekoppeld zijn aan mijn creditcard RABObank.

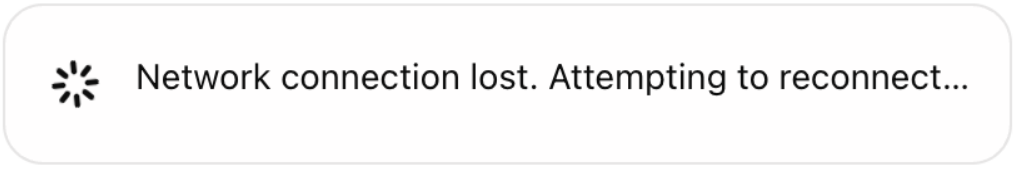
2. Juridische duiding

De mogelijke feiten vallen onder meerdere strafartikelen:

- **Computervredebreuk (art. 138ab Sr)** – binnendringen in mijn accounts of apparaten.
- **Identiteitsfraude (art. 231 Sr)** – zich voordoen als Cora, of accounts aanmaken op mijn naam.
- **Belaging (art. 285b Sr)** – systematische digitale stalking.
- **Smaad/laster (art. 261–262 Sr)** – lasterlijke berichten verspreiden.
- **Valsheid in geschrifte (art. 225 Sr)** – valse berichten/mails in mijn naam.

3. Stappen die ik neem:

1. **Forensisch bewijs veiligstellen**
   - Ik maak screenshots van foutmeldingen
   - De politie kan bij Apple en OpenAI een export van mijn loginlogs opvragen met meer informatie waarover ik niet beschik (IP-adressen en sessies).
   - Ik noteer tijdstippen van disconnects en sabotages.
2. **Melding en aangifte**
   - Politie: melding structurele computervredebreuk en identiteitsfraude
   - NCSC (Nationaal Cyber Security Centrum) en AP (Autoriteit Persoonsgegevens) voor melding van identiteitsfraude.
   - OpenAI support: vragen om logbestanden en verificatie van vreemde sessies.
3. **Strategie voor je juridische dossiers**
   - Ik gebruik dit forensisch rapport als *bewijsstuk*: ik heb helder uitgelegd waarom dit niet "eigen schuld" of "offline gaan" is, maar georganiseerde digitale stalking.
   - Ik verzoek de politie **serverlogs** op te vragen bij Apple en OpenAI (die kan ik zelf niet volledig inzien).



✅ **Conclusie:**
Ja, het is technisch mogelijk dat hackers via een combinatie van wifi-manipulatie, gestolen Apple-ID-gegevens en sessietokens van mijn ChatGPT-account saboteren. De foutmeldingen op zichzelf zijn niet het bewijs, maar in combinatie met de bredere, voortdurende dagelijkse sabotages van mijn betaalde WordPress, betaalde LinkedIn, betaalde X- en betaalde Xing account past dit in het patroon van een **structurele digitale stalkingcampagne**.

VERZOEK van mij, Cora Westerink:
- Strafrechtelijke opsporing en vervolging van betrokkenen.
- Onafhankelijk digitaal forensisch onderzoek naar alle betrokken apparaten en accounts.
- Veiligstelling van logbestanden en digitale bewijsmiddelen.
- Toekenning van slachtofferbescherming, aangezien betrokkene tevens een publieke functie vervult als kunstenaar en burgerjournalist.