Cyberoszustwa z wykorzystaniem sztucznej inteligencji

Dzięki zaawansowanym algorytmom, cyberprzestępcy mogą analizować dane szybciej i dokładniej, generować przekonujące fałszywe treści oraz automatyzować ataki na dużą skalę.

Najpopularniejsze cyberoszustwa wykorzystujące sztuczną inteligencję

1. **DEEPFAKE**
   tworzenie realistycznych, ale fałszywych obrazów i nagrań wideo
2. **PHISHING**
   wspierany przez sztuczną inteligencję (spersonalizowany i trudniejszy do rozpoznania)
3. **BOTY I AUTOMATYZACJA ATAKÓW**
   większa skala działania przestępców
4. **SOCJOTECHNIKA**
   wspierana przez sztuczną inteligencję (większa siła ataków m.in. poprzez tworzenie fałszywych tożsamości, automatyzację interakcji)

Jak rozpoznać deepfake?

Krytyczne podejście

- Zawsze weryfikuj źródło informacji.
- Uważaj na sensacyjne i szokujące doniesienia.

Nie daj się ponieść emocjom

- Treści wzbudzające strach lub presję mogą być próbą oszustwa.
- Uważaj na super oferty ograniczone czasowo bądź produkty reklamowane przez znane osoby. Nie ulegaj presji.

Weryfikacja nadawcy/ rozmówcy

- Sprawdź, kto naprawdę się z Tobą kontaktuje.
- Zadaj dodatkowe pytania, by potwierdzić tożsamość rozmówcy.

Błędy w nagraniach i obrazach

- Nienaturalne modulacje głosu, błędy w wymowie.
- Uważaj na brak synchronizacji dźwięku z ruchami ust.
- Zwracaj uwagę na nienaturalne ruchy twarzy, dodatkowe elementy na zdjęciach, rozmazane usta.

Pamiętaj!

Bądź świadomy zagrożeń, na jakie możesz się natknąć w sieci. Edukuj siebie i pracowników!

NASK
EUROPEJSKI MIESIĄC CYBER BEZPIECZEŃSTWA
PROJEKT FINANSOWANY ZE ŚRODKÓW MINISTRA CYFRYZACJI