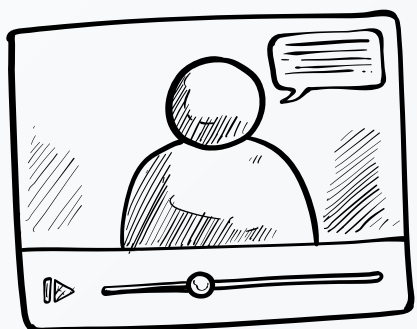


AI w rękach oszustów – uważaj na deepfake!

Jak oszuści wykorzystują AI?



- Tworzą realistyczne treści i prowadzą „profesjonalne” rozmowy.
- Podszywają się pod doradców, ekspertów lub znajomych.
- Wykorzystują deepfake: fałszywe nagrania i reklamy ze znanymi osobami, by zachęcać do inwestycji.

Każdy ślad w sieci to podpowiedź dla oszustów



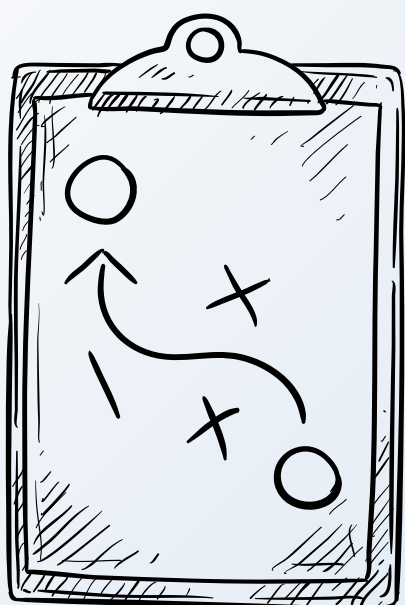
- Twoje zdjęcia, wpisy i reakcje mogą pomóc im w przygotowaniu ataku.
- Im mniej danych udostępniasz, tym trudniej Cię zmanipulować.

Najczęstsze oszustwa deepfake



- Reklamy z celebrytami zachęcającymi do fałszywych inwestycji.
- Fałszywe „wywiady” w telewizji z udziałem znanych osób.
- Podszywanie się pod znajomych proszących o pomoc finansową

Jak rozpoznać deepfake?



- Nierealistyczne ruchy twarzy – usta nie pasują do słów, brak naturalnej mimiki.
- Nienaturalny głos – płaski, robotyczny albo niepasujący do tonu wypowiedzi.
- Tło i światło – elementy wyglądają sztucznie, czasem się „rozmażają”.
- Presja emocji – obietnice „pewnego zysku” czy „oferty tylko dziś”.
- Błędy językowe – błędne odmiany, literówki, nienaturalne słowa.

Zanim uwierzysz w nagranie z celebrytą polecającym inwestycję – upewnij się, że to nie sprytna pułapka.



EUROPEJSKI
MIESIĄC
CYBER
BEZPIECZEŃSTWA

Więcej informacji na stronie
bezpiecznymiesiac.pl

WARSZAWSKI
INSTYTUT
BANKOWOŚCI

NASK