**Czym jest deepfake i jak go rozpoznać?**

**W świecie zdominowanym przez media cyfrowe, zdolność do odróżniania prawdy od fikcji staje się coraz bardziej wartościowym elementem naszego życia. W ostatnich latach narzędziem, które znacząco zaburzyło nasze postrzeganie rzeczywistości, stał się tzw. “deepfake”. Co to takiego i czy da się uniknąć wpadnięcia w jego pułapkę?**

**Czym jest deepfake?**

Termin "deepfake" wywodzi się z połączenia słów "deep learning" oraz "fake" (fałszywy). Technologia ta korzysta z głębokich sieci neuronowych **w celu tworzenia nieprawdziwych, ale zaskakująco realistycznych materiałów wizualnych**. To metoda opierająca się na sztucznej inteligencji, wykorzystująca mechanizmy uczenia maszynowego do produkowania lub modyfikowania obrazów i filmów w taki sposób, by trudno było je rozróżnić od oryginałów. W efekcie otrzymujemy nierealne klipy, które potrafią ukazywać zmyślone sceny lub zniekształcać prawdziwy obraz rzeczywistości.

Podstawą deepfake są skomplikowane sieci neuronowe. Te cyfrowe modele, inspirowane budową ludzkiego mózgu, uczą się na bazie obszernych zestawów danych, takich jak wideo, zdjęcia czy zapisy dźwiękowe. Przetwarzając te informacje, algorytmy są w stanie rozpoznać i naśladować subtelne niuanse ekspresji twarzy, modulacji głosu czy ruchów ciała. Na podstawie zdobytych w ten sposób danych powstają materiały, które choć wyglądają prawdziwie, w rzeczywistości są tworem sztucznym.

**Czy deepfake jest niebezpieczny?**

**Technologie stojące za deepfake mają zdolność do zakłócania naszego rozumienia prawdy.** Przez nie możemy obserwować scenariusze, które w rzeczywistości nie miały miejsca lub dostrzegać postacie w kontekstach, w których te nigdy się nie znalazły. Otwiera to drzwi do niezliczonych manipulacji, zarówno niewinnych, jak i potencjalnie szkodliwych. W erze "fake news", możliwość tworzenia tak realistycznych fałszywych materiałów wideo i audio stanowi kolejne wyzwanie dla krytycznego myślenia i weryfikacji faktów, zwłaszcza jeśli deepfakes są celowo używane do celów dezinformacyjnych.

*Sprawdź:* [Konsulting i audyty IT](https://cyberszkolenia.pl/konsulting-i-audyty-it/)

**Jakie zagrożenia niesie ze sobą deepfake?**

Deepfake, choć jest imponującym osiągnięciem technologicznym, niesie ze sobą wiele potencjalnych zagrożeń. Zaliczają się do nich:

l **Dezinformacja i fałszywe wiadomości:** Jedna z największych obaw dotyczących deepfake polega na możliwości tworzenia materiałów wideo lub audio, które przedstawiają fałszywe informacje. Takie materiały mogą być wykorzystywane do wprowadzania w błąd opinii publicznej, manipulowania wyborcami lub szkodzenia reputacji wybranych jednostek.

l **Szantaż i wymuszenie:** Zaawansowane deepfakes mogą być wykorzystywane do tworzenia kompromitujących nagrań, które nigdy nie miały miejsca. W rezultacie wybrane osoby mogą być narażone na szantaż lub wymuszenie.

l **Manipulacja dowodami sądowymi:** Fałszywe nagrania mogą być przedstawiane jako "prawdziwe" dowody w sprawach sądowych, co stanowi zagrożenie dla praworządności.

l **Zakłócenie zaufania do mediów:** W świecie, w którym deepfakes stają się coraz bardziej przekonujące, zaufanie do materiałów wideo i audio może zostać zachwiane. Ludzie mogą zacząć wątpić w autentyczność każdego nagrania, które widzą lub słyszą.

l **Ataki na osoby publiczne:** Politycy, celebryci i inne znane osoby są szczególnie narażone na ataki przy użyciu technologii deepfake. Fałszywe nagrania mogą być używane do dyfamacji, kreowania negatywnego wizerunku lub wprowadzenia w błąd opinii publicznej.

l **Finansowe oszustwa:** Technologia deepfake może być wykorzystywana do oszustw finansowych, np. poprzez naśladowanie głosu osób wysoko postawionych w celu wprowadzenia pracowników w błąd i nakłonienia ich do nieautoryzowanych transakcji.

l **Zagrożenia dla prywatności:** Deepfake może być wykorzystywane do inwazji prywatności, tworząc wizualne i dźwiękowe symulacje interakcji prywatnych, które nigdy nie miały miejsca.

Zważywszy na powyższe zagrożenia, konieczne jest przyjęcie środków ostrożności oraz rozwijanie narzędzi i strategii do rozpoznawania i przeciwdziałania deepfakes w różnych obszarach życia.

**Jak rozpoznać deepfake?**

Rozpoznawanie materiałów deepfake od autentycznych treści stało się jednym z kluczowych wyzwań w dziedzinie [cyberbezpieczeństwa](https://cyberszkolenia.pl/inzynieria-spoleczna-kontra-cyberbezpieczenstwo/). Choć identyfikacja manipulacji jest trudna, naukowcy i technolodzy opracowują strategie, by ułatwić ten proces. **Głęboka analiza ekspresji oraz ruchów twarzy w materiale może uwydatnić nieścisłości – przykładowo, niestosowne gesty, niewłaściwe ruchy oczu czy niespójności w mimice.**

Przestudiowanie szczegółów filmu, takich jak jakość obrazu, detale tła, a nawet cienie, może dostarczyć wskazówek o jego autentyczności. Często deepfakes zostawiają drobne "ślady", które ujawniają ich pochodzenie.

Porównując podejrzane materiały z oryginałami od przedstawionej na nich osoby, istnieje szansa na dostrzeżenie subtelnych różnic. Mogą dotyczyć one tonu głosu, sposobu mówienia czy nawet postawy ciała. Istnieją także zaawansowane programy komputerowe zaprojektowane specjalnie do wykrywania deepfakes. Wykorzystują one analizę głęboką, szukając anomalii, takich jak nieprawidłowo odbite światło czy niewyraźne granice obiektów.

**Kiedy natrafiamy na podejrzany materiał wideo w mediach społecznościowych czy na innych platformach udostępniających treści, kluczowe jest dokładne sprawdzenie źródła jego pochodzenia.** Materiały z nieznanych lub podejrzanych stron zawsze powinny budzić nasz niepokój.

Ostatecznie, w miarę jak technologia deepfake staje się coraz bardziej zaawansowana, istotne jest, aby społeczeństwo było regularnie o tym informowane i przygotowywane. **Edukacja i świadomość są kluczem do obrony przed manipulacją**. Dlatego też sektor prywatny, instytucje edukacyjne i rządy powinny współpracować w zakresie badań i opracowywania narzędzi służących do wykrywania i zwalczania deepfakes.