Warto wiedzieć…

Deepfake

Nowe wyzwania dla ochrony danych osobowych i bezpieczeństwa

Deepfake to technologia wykorzystująca sztuczną inteligencję, która pozwala na tworzenie fałszywych, ale bardzo realistycznych obrazów, filmów lub dźwięków. Może sprawiać wrażenie, że ktoś powiedział lub zrobił coś, co w rzeczywistości nigdy nie miało miejsca. Technologia ta jest niestety również wykorzystywana w działalności przestępczej, kradzieży tożsamości, wyłudzeniach pieniędzy lub danych osobowych.

Przykłady zagrożeń:

- może kogoś ośmieszyć lub skrzywdzić np. przez przerabianie zdjęć konkretnej osoby,
- może być używana do oszukiwania ludzi np. do tworzenia fałszywych wiadomości lub podszywania się pod kogoś w celu wyłudzenia danych osobowych lub pieniędzy,
- może stać się narzędziem hejtu, szantażu lub zastraszania,
- może sprawić, że trudno odróżnić to, co prawdziwe, od tego co zostało zmanipulowane.

Jak rozpoznać deepfake? Zwróć uwagę na szczegóły m.in:

- twarz, która wygląda nienaturalnie, jest zniekształcona lub „nie pasuje” do reszty ciała,
- ruchy ust, które nie pokrywają się z tym, co słyszysz,
- ruchy ciała, które mogą być bardzo nienaturalne lub nierealistyczne,
- źródło pochodzenia nagrania – sprawdź, czy materiał pochodzi z wiarygodnego i zaufanego źródła,
- treść, która brzmi nierealnie, absurdalnie albo sprzecznie z tym, co wiesz o świecie.

Jak bezpiecznie korzystać z takich narzędzi?

- nie używaj zdjęć prawdziwych osób,
- nie twórz materiałów, które kogoś ośmieszają lub mogą przestraszyć,
- jeśli tworzysz deepfake na potrzeby zabawy – wyraźnie zaznacz, że materiał jest fałszywy.

Technologia jest narzędziem — decyduj świadomie w jakim celu jej używasz.

PAMIĘTAJ!

Technologia deepfake może być wykorzystana w zarówno dobrych, jak i złych celach. Z jednej strony może pomóc np. w poprawie jakości produkcji filmowych i dźwiękowych. Z drugiej jednak – może służyć do tworzenia fałszywych treści, które szerzą dezinformację. Należy pamiętać, że nie wszystko, co znajduje się w internecie, jest prawdziwe, a wiele deepfake’ów do złudzenia przypomina prawdziwe materiały. Jeśli coś wzbudza Twoje wątpliwości lub niepokój - porozmawiaj o tym z osobą dorosłą.

Warto wiedzieć…

Trudne słowa – proste wyjaśnienia

Co oznaczają słowa, które pojawiają się w poradzie?

- **Deepfake** - to technologia wykorzystująca sztuczną inteligencję do tworzenia fałszywych, ale bardzo realistycznych obrazów, filmów lub dźwięków w celu pokazania czegoś, co nigdy się nie wydarzyło. Wykorzystując do tego techniki uczenia (deep learning) i fałszowania (fake).

- **Deepfake audio** - koncentruje się na manipulacji dźwiękiem i ludzkim głosem. Za pomocą tej technologii można tworzyć fałszywe nagrania głosowe, w których osoba wydaje się mówić lub śpiewać coś, czego w rzeczywistości nie powiedziała lub nie zaśpiewała. Deepfake audio jest często wykorzystywany w tworzeniu fałszywych nagrań rozmów telefonicznych lub przemówień.

- **Deepfake video** - polega na manipulacji materiałami filmowymi, w szczególności twarzami i ciałami. Dzięki tej technologii można stworzyć nieprawdziwe materiały video. Deepfake video jest używane do różnych celów np. do manipulacji informacjami i tworzenia fałszywych treści.

- **Dezinformacja** - to celowe rozpowszechnianie fałszywych lub wprowadzających w błąd treści, informacji tzw. fake newsów. Technologia deepfake bardzo często jest wykorzystywana do tworzenia takich treści.

- **Sztuczna inteligencja** - zwana również AI (ang. Artificial Intelligence), to dziedzina informatyki zajmująca się tworzeniem maszyn i systemów, które potrafią wykonywać zadania wymagające ludzkiej inteligencji. Obejmuje to takie umiejętności jak rozumowanie, uczenie się, rozwiązywanie problemów, postrzeganie i podejmowanie decyzji.

- **Dane osobowe** - to informacje, które mogą pomóc kogoś zidentyfikować np. imię i nazwisko, adres, numer telefonu, e-mail, głos, czy wizerunek. Takich danych nie powinno się udostępniać nieznanym osobom i aplikacjom bez potrzeby.