

Rośnie cyberprzestępcstw wykorzystaniem AI

liczba
z

19 maja 2024

W internecie pojawia się coraz więcej przestępstw typu deepfake – ostrzegają eksperci z instytutu badań Naukowej i Akademickiej Sieci Komputerowej. Technika oszustw polega na wykorzystaniu głosu i twarzy znanych osób, obrobionych przy pomocy sztucznej inteligencji.



Ekspert z NASK poinformował, że w internecie pojawia się coraz więcej oszustw opartych na filmach, w których używa się wizerunku osób publicznych, jak np. piłkarz Robert Lewandowski czy minister zdrowia Izabela Leszczyna. W filmach używa się techniki synchronizacji ruchu ust, tak by sztucznie wygenerowany głos zgadzał się z ruchem ust i gestykulacją – wyjaśniono. Sam termin deepfake wynika z połączenia techniki sztucznej inteligencji „deep learning” („zaawansowane uczenie się”) oraz „fake” („fałszywy”).

W komentarzu NASK przytacza przykład z marca br., kiedy to w serwisie społecznościowym pojawił się film typu deepfake z właścicielem i prezesem firmy InPost Rafałem Brzoską. Pomimo szybkiej reakcji pokrzywdzonego i zgłoszenia sprawy do administratorów serwisu Meta, film był dostępny na platformie przez wiele dni.

„Technologie umożliwiają obecnie przestępcom łatwe manipulacje materiałami audiowizualnymi. W przypadku technologii typu »text-to-speech«, wystarczy im zaledwie kilka sekund nagranego głosu, aby stworzyć nowy podkład dźwiękowy, który może być zsynchronizowany z materiałem wideo, na przykład z dowolnego

przemówienia czy wiecu politycznego. Dla technologii »speech-to-speech«, w której intonacja, emocje zawarte w głosie są bardziej złożone, do wykonania podróbki potrzebny jest dłuższy fragment, około jednej minuty oryginalnego materiału” – wyjaśniła kierowniczka zespołu NASK ds. analizy deepfake Ewelina Bartuzi-Trokielewicz.

Eksperci przekazali, że w maju br. ponownie nastąpił wysyp filmów typu deepfake, które wykorzystują wizerunek znanych osób jak np. influencera Kamila Labuddy, prezydenta Andrzeja Dudy czy ponownie Rafała Brzowski. Jak dodali, na kradzież wizerunku i głosu są narażone osoby znane, jak np. aktorzy, celebryci czy biznesmeni oraz cieszące się zaufaniem w pewnych kręgach i traktowane jako autorytet. „Użytkownicy mediów społecznościowych powinni ostrożnie podchodzić do treści wideo, które wydają się niezweryfikowane lub podejrzane. Dotyczy to zwłaszcza tych materiałów, które mają potencjalny wpływ na publiczne postrzeganie znaczących postaci i instytucji” – przestrzegła ekspertka NASK.

Jak podkreślono, tego typu oszustwa stają się coraz trudniejsze do wykrycia. Rozwijająca się sztuczna inteligencja pozwala coraz dokładniej podkładać sztucznie wygenerowany głos, jednak eksperci zaznaczyli, że nie jest to niemożliwe. Należy oglądany film sprawdzić od strony technicznej i analizować jego przekaz.

Wśród zastrzeżeń technicznych sugerujących oszustwo eksperci wymieniają: zniekształcenie obraz w okolicy ust, problem w odwzorowaniu uzębienia, nienaturalny ruch głową i mimika, błędy w odmianie słów czy nietypową intonację. „Coraz częściej oszuści stosują też technikę dodawania szumów i różnego rodzaju plam na nagraniach, co ma na celu zakłócenie klarowności przekazu obrazu, ukrycie artefaktów generowanych przez sztuczną inteligencję oraz dezorientację algorytmów automatycznej detekcji deepfake’ów” – dodała Bartuzi-Trokielewicz.

NASK dodał, że w filmach zastosowane są różne socjotechniki mające nakłonić odbiorcę, jak np.: obietnica szybkiego zysku, wyjątkowość oferty połączona z ograniczonym dostępem w czasie, ponaglanie do działania oraz odwoływanie się do emocji odbiorcy.

W przypadku zaobserwowania takiego materiału NASK zachęca do szybkiej reakcji oraz poinformowania odpowiednich organów, które mogą uchronić innych od zostania ofiarą oszustwa. Można np. zgłosić materiał do zespołu CERT Polska poprzez sms (numer: 8080) lub stronę incydent.cert.pl. Istnieje możliwość przesłania materiału na adres mailowy instytutu (deepfake@nask.pl), który pozwoli na analizę materiału w celu opracowania możliwości zapobiegania takim praktykom w przyszłości.

Autorstwo: PAP

Źródło: [NaukawPolsce.pl](https://naukawpolsce.pl)