

Ukradli miliony dolarów imitując głos sztuczną inteligencją

9 marca 2023

Modele sztucznej inteligencji zaprojektowane tak, aby dokładnie naśladować ludzki głos, ułatwiają atakującym wyłudzenie tysięcy dolarów od wrażliwych osób. W 2022 roku oszuści byli w stanie oszukać łatwowiernych obywateli na 11 milionów dolarów w samych Stanach Zjednoczonych, udając z reguły ich bliskich krewnych.

Tymczasem wiele firm nadal aktywnie wypuszcza na rynek produkty AI, które mogą dokładnie naśladować głos na bardzo małym zbiorze danych. Kwestia kontroli takich technologii staje się coraz bardziej dotkliwa.

Według Federalnej Komisji Handlu oszuści udający krewnych ofiar są bardzo powszechni w Stanach Zjednoczonych. Było to najczęściej zgłaszane oszustwo w 2022 roku. Spośród 36 tys. wiadomości ponad 5 tys. ofiar zostało oszukanych na 11 milionów dolarów przez telefon. Ponieważ osoby atakujące mogą znajdować się w dowolnym miejscu na świecie, władzom trudno jest powstrzymać niewłaściwe postępowanie i odwrócić niepokojący trend.

Niektóre programy do tworzenia głosu wspomagane przez sztuczną inteligencję wymagają tylko kilku zdań dźwiękowych, aby w przekonujący sposób odtworzyć mowę mówcy z niezbędnymi emocjami. Ofiarom oszustw, a są to często osoby starsze, coraz trudniej jest stwierdzić, czy głos został sfałszowany. Na przykład jedna para wysłała oszustowi 15 tys. dolarów za pośrednictwem terminala Bitcoin, wierząc, że rozmawiają z ich synem. Głos wygenerowany przez sztuczną inteligencję powiedział, że potrzebuje pieniędzy na opłaty prawne po tym,

jak miał wypadek samochodowy, w którym zginął amerykański dyplomata.

Prawdopodobnie najlepszą obroną jest podnoszenie świadomości na temat nowego rodzaju oszustwa opartego na symulacjach głosowych. Wszelkie prośby o gotówkę należy traktować ze sceptycyzmem. Przed wysłaniem środków lepiej spróbować skontaktować się z osobą, która rzekomo prosi o pomoc w inny sposób niż połączenie głosowe.

Możliwość łatwego tworzenia przekonujących symulacji głosu już wywołała kontrowersje. Na przykład członkowie grupy 4chan wyrażali celebrytów rasistowskimi, obraźliwymi lub brutalnymi wypowiedziami. W tym momencie stało się jasne, że firmy muszą pomyśleć o dodatkowych środkach ochrony, aby zapobiec niewłaściwemu wykorzystaniu technologii. W przeciwnym razie ryzykują pociągnięciem do odpowiedzialności za szkody, takie jak utrata reputacji.

Sądy nie zdecydowały jeszcze, czy firmy będą odpowiadać za szkody wyrządzone przez technologię głosową deep fake lub jakąkolwiek inną technologię sztucznej inteligencji. Można wywierać jednak presję na sądy i organy regulacyjne, aby kontrolowały rynek sztucznej inteligencji. Wiele firm nadal wypuszcza na rynek produkty AI, nie zdając sobie w pełni sprawy ze związanego z tym ryzyka. Niedawno Microsoft wprowadził nową funkcję w wersji testowej Bing AI, która może służyć do naśladowania głosu celebrytów. Jednak to, co te głosy mogą powiedzieć, ogranicza się do niewielkiej liczby tematów. Najwyraźniej w ten sposób Microsoft stara się uniknąć skandali.

Źródło: [ZmianyNaZiemi.pl](https://zmiany.naziemi.pl)