



Sztuczna Inteligencja pomaga w oszustwach „na wnuczka”

2026-08-24

Dzwoni telefon. W słuchawce słyszymy wnuczka. Jest wyraźnie zdenerwowany, mówi szybko, opowiada o wypadku i prosi o pilną pomoc finansową. Do tego nalega, żeby na razie nikomu o tym nie mówić. Głos brzmi znajomo, sposób mówienia też... Ale dzisiaj nie daje to pewności, że naprawdę rozmawiamy z bliską osobą.

Sztuczna inteligencja potrafi coraz lepiej naśladować ludzki głos. Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy (NASK) ostrzega, że do stworzenia takiej imitacji może wystarczyć nawet kilka sekund nagrania. Próbką głosu może pochodzić z filmu zamieszczonego w mediach społecznościowych, relacji albo wiadomości głosowej wysłanej przez komunikator.

Program analizuje barwę głosu, tempo mówienia, intonację i charakterystyczny sposób wypowiadania słów. Później może wygenerować zupełnie nową wypowiedź, która brzmi tak, jakby powiedziała ją konkretna osoba.

„Babciu, miałem wypadek”

Sam scenariusz oszustwa nie jest nowy. Od lat zdarzają się telefony, podczas których ktoś podaje się za wnuka, córkę, syna albo inną bliską osobę. Opowiada o wypadku, zatrzymaniu przez policję lub nagłym problemie i przekonuje, że pieniądze są potrzebne od razu.

Nowością jest to, że oszust nie musi już liczyć wyłącznie na to, że uda mu się dobrze odegrać rolę. Może spróbować wykorzystać narzędzia, które naśladowują prawdziwy głos.

Do tego może wcześniej poszukać informacji o rodzinie. Imiona bliskich, zdjęcia, informacje o wyjazdach, pracy czy miejscu zamieszkania często sami zostawiamy w internecie. Jeśli rozmówca zna kilka takich szczegółów, cała historia może zabrzmieć jeszcze bardziej przekonująco.

Wygenerowany głos może być nienaturalny

Czasami można zauważyć coś nienaturalnego. Głos może być zbyt równy, mogą pojawić się nietypowe pauzy, zmiany tempa, nienaturalna intonacja albo lekko mechaniczne brzmienie.

Problem w tym, że nie zawsze takie różnice będą wyraźne. A kiedy na początku rozmowy słyszymy o wypadku, szpitalu czy innym nieszczęściu, trudno spokojnie analizować każde słowo.

Dlatego lepiej nie próbować rozstrzygać przez telefon czy głos jest prawdziwy. Najprostsze rozwiązanie jest też najbezpieczniejsze: **rozłączyć się i samemu zadzwonić do osoby, która rzekomo potrzebuje pomocy.**

Jeżeli rzeczywiście coś się wydarzyło, kilka minut poświęconych na sprawdzenie informacji niewiele



zmieni. Jeśli natomiast dzwonił oszust, taki prosty krok może uchronić nas przed utratą pieniędzy.

Rodzinne hasło może się przydać

Policja radzi również, aby ustalić z najbliższymi proste hasło bezpieczeństwa. Nie chodzi oczywiście o hasło do banku czy telefonu, ale o zwykłe słowo albo krótkie zdanie znane tylko rodzinie. Gdy ktoś zadzwoni z nietypową, pilną prośbą, można poprosić go o podanie takiego hasła.

Lepiej jednak nie wybierać czegoś łatwego do odgadnięcia. Imię psa, data urodzenia czy miejsce, do którego co roku jeździmy na wakacje, mogą być widoczne w mediach społecznościowych. Bezpieczniejsze będzie coś zupełnie przypadkowego.

Kiedy powinna zapalić się czerwona lampka?

W takich rozmowach często powtarzają się podobne zdania:

- „Musisz zrobić przelew natychmiast”.
- „Nie mów o tym nikomu”.
- „Nie dzwoń teraz do mamy”.
- „Podaj mi kod BLIK”.
- „Policjant zaraz przyjedzie po pieniądze”.
- „Nie rozłączaj się”.

Warto zwrócić uwagę przede wszystkim na pośpiech. Oszustowi zależy na tym, żebyśmy nie mieli czasu spokojnie pomyśleć, zadzwonić do kogoś z rodziny albo sprawdzić, czy historia w ogóle jest prawdziwa.

Im bardziej ktoś naciska, straszy i prosi o zachowanie wszystkiego w tajemnicy, tym większa powinna być nasza ostrożność.

Co zrobić po podejrzanym telefonie?

Przede wszystkim nie należy przekazywać pieniędzy ani podawać loginów, haseł, kodów autoryzacyjnych czy kodów BLIK. Nie powinniśmy też oddawać gotówki osobie, która ma rzekomo przyjść po nią w imieniu wnuka, policjanta czy prawnika.

Najlepiej zakończyć rozmowę i samodzielnie zadzwonić do osoby, której sprawa ma dotyczyć. Jeśli nie odbiera, można skontaktować się z innym członkiem rodziny i spokojnie wszystko sprawdzić. Nie ma nic złego w tym, że przed udzieleniem pomocy chcemy upewnić się, co naprawdę się wydarzyło.

Nie każde takie oszustwo wykorzystuje sztuczną inteligencję



**Magiczny
Kraków**

Warto też zachować proporcje. Sztuczna inteligencja daje oszustom nowe możliwości, ale nie oznacza to, że każdy podejrzany telefon wykorzystuje sklonowany głos.

NASK zwraca uwagę, że nadal bardzo częste są znacznie prostsze metody: fałszywe SMS-y, wiadomości z przejętych kont, podszywanie się pod znajomych w komunikatorach czy próby wyłudzenia kodów BLIK.

Technologia się zmienia, ale sposób działania przestępców pozostaje podobny. Najpierw próbują wzbudzić strach, potem wywierają presję, a na końcu proszą o pieniądze.