

Oszuści telefoniczni klonują głos ofiary

31 lipca 2020

Jednym z dziwacznych zastosowań deepfakes, technologii sztucznej inteligencji używanej do manipulowania treściami audiowizualnymi, jest oszustwo audio. Hakerzy używają uczenia maszynowego do klonowania czyjegoś głosu, a następnie łączą ten klon głosu z technikami inżynierii społecznej. Daje to oszustom możliwość przekonania ludzi do transferu środków tam, gdzie ich nie ma.

Takie oszustwa były skuteczne w przeszłości, ale jak dobre są klony głosu używane w tych atakach? Tak naprawdę nigdy nie słyszeliśmy o oszustwie dźwiękowym. Jeszcze nie...

Firma konsultingowa NISOS, zajmująca się bezpieczeństwem, opublikowała raport, w którym przeanalizowano jedną z prób oszustw telefonicznych i udostępniła fragment dźwięku. W nagraniu słychać głos podobny do głosu prezesa firmy, proszący pracownika o „natychmiastową pomoc w wykonaniu pilnej transakcji biznesowej”. To jest fragment wiadomości głosowej, którą otrzymał pracownik firmy technologicznej. Nazwa firmy nie została ujawniona.

Jakość z pewnością nie jest świetna. Nawet pod pozorem złego sygnału telefonicznego słychać, że głos jest trochę robotyczny. To jednak można znieść, bo gdybyś był młodszym pracownikiem i denerwował się po otrzymaniu rzekomo pilnej wiadomości od szefa, być może nie zastanawiałbyś się zbyt nad jakością dźwięku.

Atak ostatecznie się nie powiódł, ponieważ pracownik odbierający wiadomość głosową od razu pomyślał, że jest podejrzana i wysłał ją do działu prawnego firmy. Ale takie ataki staną się bardziej powszechne, gdy bardziej dostępne

będą głęboko fałszywe narzędzia.

Wszystko, czego potrzebujesz, aby utworzyć klon głosu, to dostęp do wielu nagrań celu. Im więcej masz danych i im lepsza jakość dźwięku, tym lepszy będzie wynikowy klon głosu. Dla wielu prezesów dużych firm takie taśmy można łatwo skompilować na podstawie rozmów telefonicznych, wywiadów i wystąpień publicznych. Mając wystarczająco dużo czasu i danych, dźwięk najwyższej jakości będzie znacznie bardziej przekonujący niż w powyższym przykładzie. Oczywiście jest, że oszuści telefoniczni osiągnęli nowy poziom, a jakość oszustw będzie tylko rosła.

Na początku tego roku FTC ostrzegała przed wzrostem liczby takich oszustw, ale eksperci twierdzą, że jest jeden łatwy sposób na ich pokonanie. Wszystko, co musisz zrobić, to rozłączyć się i oddzwonić do tej osoby.

„Rozłącz się i oddzwoń. Jeśli nie jest to bardzo, bardzo wyrafinowana grupa hakerów, jest to prawdopodobnie najlepszy sposób, aby dowiedzieć się, czy rozmawiałeś z kimś, kogo uważasz za wiarygodnego interlokutora”.

Autorstwo: tallinn

Źródło: ZmianyNaZiemi.pl