

# UMĚLÁ INTELIGENCE UMÍ NAPODOBIT I HLAS. K podvodu stačí jen pár vteřin jeho záznamu, varují vědci

- CZ24 News | 15. dubna 2023

**ČESKO: Ukrást se dá téměř cokoliv, dokonce i lidský hlas. Upozorňují na to brněnští vědci z Vysokého učení technického. Ve svých výzkumech dokázali, že k nasimulování hlasu podvodníkům stačí jen pár vteřin záznamu. Vědci proto řeší, jak takovému falšování zabránit. A varují před tím, že nemůžeme věřit všemu, co slyšíme na internetu nebo v telefonu.**



Kamil Malinka (vpravo) a Anton Firc | Foto: Ondřej Vaňura | Zdroj: Český rozhlas

„To jsem nahrál, a teď ten model zase necháme zpracovat tu změnu,“ říká Anton Firco, doktorand na Ústavu inteligentních systémů na Vysokém učení technickém. U malého notebooku spolu právě zkoušíme napodobit můj hlas.

„Jsem Ondřej Vaňura z Českého rozhlasu. Rád bych od vás obdržel milion.“ Tak zní věty, které software vytvořil za necelou minutu. Rozhodně to není geniální, ale jde o něco, co jsem ve skutečnosti vůbec neřekl.

„Ano, samozřejmě, toto byl velmi naivní scénář, který byl velmi rychle sestaven, a tomu odpovídá i kvalita. Když bych si dal víc práce a nasbíral si k tomu 20 minut stopáže vaší řeči, je možné ten model trochu dotrénovat a výsledek bude o mnoho lepší,“ vysvětluje Firc.

Takže ve chvíli, kdy jsou v rozhlasovém online archivu hodiny záznamů s mým hlasem, navíc v dobré kvalitě, by bylo napodobení o dost věrohodnější. Podstatně lépe systém zvládá třeba hlas představitele Jamese Bonda, herce Daniela Craiga.

## Hlasové podvody

„Jde o algoritmy, které se používají pro syntézu řeči. Konkrétně v tomto případě jsou schopné pomocí nahrávky napodobit váš hlas. Jde o speciální přístup ve strojovém učení, takzvaný one shot nebo shot learning,“ vysvětluje vědec Anton Firc, jak podobné systémy fungují.

Brněnští experti téma zkoumají několik let. A zmapovali už i hlasové podvody, které se staly v zahraničí.

„První útoky byly tak dva až tři roky zpátky. Opravdu tam byl jeden hovor, kdy v rámci firmy měli nastavené nějaké procesy, že CEO zavolá ekonomce, přes telefon potvrdí nějakou velkou částku, která pak odejde. Toho využil útočník. To znamená, že znal prostředí té firmy, provedl falešný hovor,“ říká mi Kamil Malinka, který působí jako odborný asistent na Vysokém učení technickém v Brně.

Vědci vidí hrozbu do budoucna. Kvůli stále lepším a lepším technologiím budou totiž dokonalejší i hlasové systémy.

„A navíc se nám to zrychluje. To znamená, že poměrně brzo můžeme být ve stavu, kdy já si zapnu nějaký filtr na platformě jako MS Teams, zapnu si jiný hlas, zapnu si jiný zvuk, a můžu se krásně vydávat za vás,“ upozorňuje. Jak se ale proti takovým podvodům bránit?

„Je potřeba být více obezřetný při tom, co děláte. To znamená, že když vám volá babička, že ji někdo drží, a potřebujete někam poslat milion korun, tak je potřeba zavěsit, zavolat babičce a zeptat se ,babičko, jsi to opravdu ty?‘“ říká Anton Firc.

„To znamená takové ty běžné mechaniky, které jste schopni aplikovat, když o tom víte,“ dodává. Brněnští vědci proto hledají způsoby, jak upravené hlasy co nejsnadněji odhalit.

Zpracoval: Ondřej Vaňura