Hlasové otisky nejsou bezpečné! Umělá inteligence používaná k hacknutí bankovních účtů!

infokuryr.cz/n/2023/03/09/hlasove-otisky-nejsou-bezpecne-umela-inteligence-pouzivana-k-hacknuti-bankovnich-uctu

kuryr 9. března 2023

Než umělá inteligence mohla duplikovat lidský hlas, hlasové otisky byly považovány za jedinečné. No, jsou jedinečné, ale nový software AI je dokáže „zfalšovat“ do té míry, že zní stejně jako vy. I banky se dají oklamat. Není zde prokazatelně potřeba duplikace hlasu, ale to nezabránilo programátorům Technocrat v jejím vývoji. - Editor TN

- Software pro generování hlasu AI lze použít k replikaci hlasů a získání přístupu k bankovním účtům.
- Pomocí tohoto softwaru byl prolomen program Voice ID Lloyds Bank.
- Kdokoli, kdo má přístup k hlasovým nahrávkám, mohl použít software pro generování hlasu AI k hacknutí bankovních účtů.

Technologický autor nedávno objevil, že software pro generování hlasu AI lze použít k obejití bezpečnostních opatření bankovních účtů. Software byl použit k replikaci syntetického hlasu, který měl přístup k informacím o účtu, včetně zůstatků na účtech a nedávných transakcí. Tento článek se zabývá nebezpečím softwaru pro generování hlasu AI, jeho používáním a kroky, které mohou banky podniknout, aby zabránily podvodným aktivitám.

Nebezpečí softwaru pro generování řeči AI

Software pro generování řeči AI dokáže generovat syntetické hlasy schopné mluvit jakýmkoli textem napsaným na webu. To představuje riziko pro všechny, protože kdokoli s přístupem k hlasové nahrávce by mohl použít software k replikaci něčího hlasu a získat přístup k citlivým informacím.

Joseph Cox, technický spisovatel pro Vice, nedávno testoval bezpečnostní opatření automatické servisní linky své banky pomocí klipu, který vytvořil pomocí nástroje pro vytváření hlasu AI. Během několika sekund měl přístup k informacím o svém účtu, včetně zůstatku a nedávných transakcí. Později totéž zkusil s účtem v Lloyds Bank, kde jeho první pokus selhal, ale poté, co nechal software číst delší texty, aby dodal kadenci důvěryhodnost, se mu podařilo získat přístup.

Jak funguje software pro generování řeči AI?

Chcete-li použít software pro generování umělého hlasu, osoba nahraje několik minut své řeči a nahraje ji do softwaru. Software poté vygeneruje syntetický hlas, který dokáže vyslovit zadaný text. Software se snadno používá a postrádá robustní bezpečnostní opatření, která by zabránila zneužití.

Banky používají technologii hlasového ověřování

Mnoho bank, včetně Wells Fargo, TD Bank a Chase, používá technologii hlasové autentizace, aby umožnila svým zákazníkům provádět bankovní transakce po telefonu, jako je kontrola jejich účtů. B. dotazování zůstatků na účtech a transakční historie nebo převodů. Lloyds Bank se chlubí, že její program Voice ID je bezpečný a jedinečný pro každého člověka, analyzuje více než 100 charakteristik, ale zjevně nedokáže rozlišit mezi lidskými a uměle generovanými hlasy.

Možné důsledky

S nástroji umělé inteligence, které se vyvíjejí a zdokonalují rychlým tempem, mohou být autentizační opatření, která se nyní zdají být špičková, brzy snadno prolomitelná. Rachel Tobac, generální ředitelka SocialProofSecurity, doporučuje, aby společnosti využívající hlasové ověřování co nejdříve přešly na bezpečnější metodu ověřování identity, jako je vícefaktorová autentizace. Technologie generování hlasu AI umožňuje proniknout do něčího účtu, aniž byste s ním kdy v reálném životě interagovali.

ZDROJ


celonárodní setkání
přijďte podpořit
ČESKO PROTI BÍDĚ
11. 3. 2023 / 14.00 hod.
VÁCLAVSKÉ NÁMĚSTÍ
vystoupí:
JINDŘICH RAJCHL - předseda PRO / JANA ZWYRTEK HAMPLOVÁ - senátorka
VIDLÁK - blogger / a mnozí další

Sdílet: