Nová technologie odposlechu Google by mohla přimět vlády, aby nařídily skenování zařízení

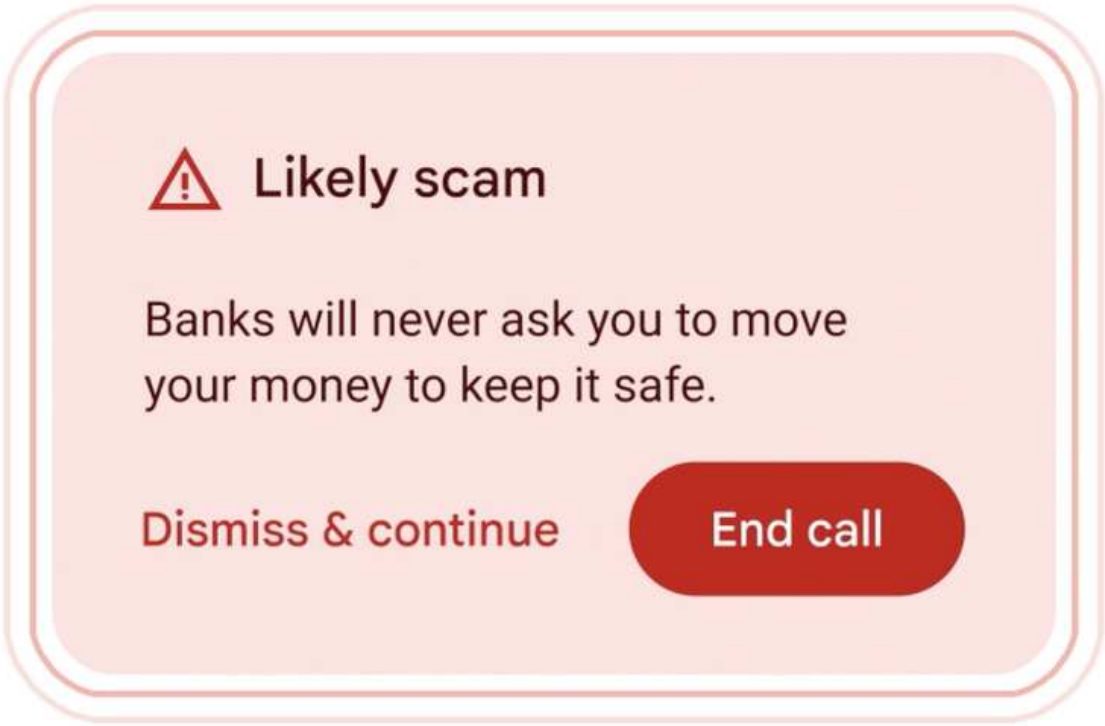
infokuryr.cz/n/2024/05/19/nova-technologie-odposlechu-google-by-mohla-primet-vlady-aby-naridily-skenovani-zarizeni

kuryr 19. května 2024

Digitální podvody jsou stále sofistikovanější a nejnovější inovace společnosti Google nabízí slibný ochranný mechanismus. Ale stejně jako u všeho, co Google propaguje jako pokrok, dopad na život a důsledky této technologie by se mohly stát velkým problémem pro občanské svobody.

Jak bylo oznámeno na vývojářské konferenci I/O, společnost testuje novou funkci sledování hovorů, která má chránit uživatele Androidu před podvody s telefony. Tato funkce využívá Gemini Nano, zjednodušenou verzi velkého hlasového modelu Gemini od Googlu, který může běžet lokálně na zařízeních, aby detekoval podvodný jazyk a vzory v hovorech a upozornil uživatele v reálném čase. Tento vývoj je důležitým krokem v boji proti podvodům, ale také vyvolává kritické otázky týkající se ochrany údajů a potenciálu širších aplikací, které by mohly porušovat osobní svobody.

Gemini Nano: Mocný nástroj proti podvodům



Nová funkce Google využívá pokročilou umělou inteligenci k hledání známek podvodného chování, jako jsou: Např. žádosti o osobní údaje, urgentní převody peněz a platby dárkovými kartami. Vzhledem k tomu, že Gemini Nano funguje výhradně na zařízení, je zachováno soukromí konverzací a (teoreticky) není nutné je odesílat na externí servery ke zpracování.

Pohled EU: Od bezpečnosti dětí k možnému překračování hranic

Evropská unie stojí v čele legislativních snah o regulaci online světa, zejména s cílem chránit děti před sexuálním materiálem – nebo jej alespoň využít jako záminku k narušení soukromí. Mimo jiné návrh EU „Kontrola chatu“ vyvolal vzrušenou debatu kvůli svému dopadu na soukromí a šifrování. Původně návrh požadoval, aby technologické společnosti přijaly skenování na straně klienta (CSS) (tj. skenování na zařízení) k detekci škodlivého obsahu před jeho zašifrováním a odesláním. Mnoho kritiků tvrdí, že by to mohlo vést k hromadnému sledování, oslabit end-to-end šifrování a nakonec by to mohlo být použito ke sledování a identifikaci informátorů, disidentů nebo jiných lidí, které chce vláda sledovat.

Nová funkce detekce podvodů od Googlu se sice zaměřuje na telefonní hovory, ale vytváří precedens pro používání pokročilé umělé inteligence ke sledování obsahu v reálném čase. Některé technologické společnosti odrazily takové invazivní návrhy a návrhy narušující soukromí. Ale nyní, když se Google rozhodl implementovat tuto funkci detekce podvodů, mohly by se otevřít dveře pro další formy skenování na zařízení.

Nyní, když tato technologie existuje a je každopádně používána, by tento vývoj mohl povzbudit EU, aby rozšířila podobné požadavky na další formy komunikace, jako jsou e-maily, chaty a interakce na sociálních sítích, pod rouškou prevence různých typů škodlivého obsahu, včetně „dezinformací“. “, „nenávistné projevy“ a další aktivity. Dnes je to o podvádění, zítra o neshodách.

To ukazuje na budoucnost, kdy se lidé nebudou muset starat pouze o cloud, pokud jde o monitorování a ovládání řeči, ale také o to, zda mohou nakonec chránit své soukromí na svých vlastních zařízeních.

Obavy o soukromí a riziko skluzu

Možnost rozšíření této technologie nad rámec jejího původního účelu vyvolává značné obavy o soukromí. Pokud by EU nařídila používání skenování na straně klienta pro širší rozsah obsahu, mohlo by to vést ke scénáři, kdy budou všechny formy digitální komunikace pod neustálým dohledem. To by mohlo narušit ochranu soukromí šifrováním typu end-to-end, protože všechny zprávy by musely být před šifrováním zkontrolovány na nelegální obsah.

Kritici tvrdí, že tento přístup by mohl vést ke stavu sledování, ve kterém je osobní komunikace neustále kontrolována algoritmy AI jménem státu. Dalším vážným problémem je riziko falešných poplachů, kdy je legitimní obsah nesprávně klasifikován jako škodlivý. Takové chyby by v konečném důsledku mohly vést k

neoprávněnému sledování nevinných lidí a omezení svobody projevu, protože před sledováním disidentů není v bezpečí ani vlastní zařízení.