

Virtuální trenéři: revoluce ve fitness, ale za jakou cenu? Chraňte svá data

9.1.2025 - | PROTEXT

Sítě sociálních médií mění podobu osobního tréninku tak, že se s offline službami jednoduše nedají srovnávat. Díky poutavému obsahu, jako jsou ukázky cvičení, příběhy o úspěšných proměnách postavy nebo tipy pro zdravý životní styl, se z osobních trenérů stávají noví influenceri, kteří oslovují zájemce po celém světě a lákají své příznivce, aby jim za jejich služby platili. Očekává se, že globální trh s online fitness službami poroste až do roku 2033 ročním tempem 29,6 %.

Při registraci do takových virtuálních cvičebních programů však často dochází ke sdílení citlivých osobních údajů, jako jsou informace o zdravotním stavu, fotografie dosaženého pokroku nebo platební údaje, s někým, koho jste možná nikdy osobně nepotkali. Děje se tak obvykle prostřednictvím profilu trenéra na sociálních sítích nebo nástrojů pro zasílání zpráv, často bez jakýchkoli závazných smluv nebo odpovídajících formálních dohod. Tím se výrazně zvyšuje riziko ohrožení nebo zneužití osobních údajů uživatelů. O konkrétních případech narušení bezpečnosti v souvislosti s online službami osobního tréninku se zatím příliš neinformovalo, ale do hledáček médií se už kvůli podobným incidentům dostaly některé fitness aplikace. Vzhledem k paralelám mezi fitness aplikacemi a virtuálními trenéry je tedy rozhodně na místě zvýšená obezřetnost uživatelů.

Mezi formy zneužití údajů v této souvislosti patří mimo jiné:

1. Možné ohrožení použitými nástroji třetích stran: Trenéři se při plánování, platbách, komunikaci a vytváření personalizovaných fitness programů často spoléhají na aplikace nebo platformy třetích stran. Pokud tyto nástroje nejsou bezpečné, mohou se stát slabými články ochrany dat.

2. Zneužití fotografií pokroku při cvičení: Fotografie z průběhu cvičení a formování postavy, které často zahrnují polonahé i zahanbující snímky, by mohly být bez souhlasu použity ke škodlivým účelům nebo uniknout na internet.

3. Rizika vydávání se za někoho jiného: Pokud je účet influencera napaden, mohou hackeři jeho jménem požadovat osobní údaje nebo platby od nic netušících sledujících.

„Osobní online tréninkové programy nemusí být ze své podstaty bezpečné, uživatelé však přesto často přehlížejí jednoduchá opatření, která by je mohla ochránit před velkými problémy,“ říká Olga Svistunova, bezpečnostní expertka společnosti Kaspersky. A dodává: „Než abyste však tyto programy zcela zavrhlí, podnikněte raději proaktivní kroky na svoji ochranu. Například:

- Ověřte si totožnost trenéra: Zjistěte si jeho pověst a kvalifikaci prostřednictvím spolehlivých fitness organizací. Podívejte se na recenze a reference ověřených klientů. Zkontrolujte, zda je jeho profil na sociálních sítích ověřený (modré zaškrtnutí nebo ekvivalentní označení).

- Neklikejte na neznámé odkazy: Nikdy neklikejte na odkazy zaslané prostřednictvím nevyžádaných zpráv nebo e-mailů, které tvrdí, že nabízejí fitness nabídky. Místo toho přejděte přímo na oficiální webové stránky trenéra nebo na důvěryhodnou fitness platformu.

- Kontrolujte HTTPS: Ujistěte se, že všechny webové stránky, na které jste přesměrováni, mají v adrese URL uvedeno HTTPS, což znamená, že jsou zabezpečené.

- Sdílejte s rozumem: Poskytujte pouze nezbytné informace a zajistěte, aby citlivé údaje, jako jsou zdravotní záznamy nebo fotografie z průběhu cvičení, byly sdíleny prostřednictvím zabezpečených a šifrovaných platforem.

- Používejte antivirový software: Spolehlivý antivirový program, například Kaspersky Premium, chrání vaše zařízení v reálném čase před viry a malwarem, blokuje škodlivé stránky, phishingové e-maily, infikované reklamy i skimmery kreditních karet vytvořené hackery za účelem krádeže vašich dat.

Tato opatření významně posilují bezpečnost a umožňují vám využívat výhod virtuálních fitness programů s větším klidem a menším rizikem možného zneužití dat.“

<https://www.ceskenoviny.cz/tiskove/zpravy/virtualni-treneri-revoluce-ve-fitness-ale-za-jakou-cenu-chrante-sva-data/2618113>