



Sport invernali e fitness tracker: l'entusiasmo per l'attività fisica può mettere a rischio i dati personali

Descrizione

COMUNICATO STAMPA - CONTENUTO PROMOZIONALE

La prossima competizione invernale potrebbe scatenare un boom del fitness, ma attenzione alla trappola rappresentata dai fitness tracker.

Con l'inizio dei giochi invernali, milioni di fan in tutto il mondo si sintonizzeranno per vedere gli atleti d'élite spingersi al limite. Questo evento mondiale annuale spesso ispira le persone a intraprendere o riprendere il proprio percorso di fitness, frequentando la palestra, monitorando gli allenamenti all'aperto o semplicemente controllando la frequenza cardiaca e altri dati biologici. Tuttavia, nella fretta di rimettersi in forma e stare bene, molti si espongono inconsapevolmente a gravi rischi per la privacy dei dati, che potrebbero portare a doxing, attacchi di phishing mirati o persino a premi assicurativi sanitari più elevati.

I dispositivi per il fitness, come smartwatch, braccialetti o anelli, possono monitorare passi, sonno e dati biometrici come l'ossigeno nel sangue o la frequenza cardiaca. Gli utenti possono inoltre inserire ulteriori informazioni sulla propria salute, come peso, gruppo sanguigno o quantità di liquidi assunti quotidianamente. Questi strumenti consentono anche di monitorare gli allenamenti all'aperto e pubblicare i dettagli delle attività fisiche, inclusi i dati GPS, per condividere i progressi con amici o familiari.

Tuttavia, la pubblicazione dei dati GPS, sia all'interno delle app fitness associate al dispositivo sia sui social network, può fornire a potenziali aggressori informazioni utili per tracciare fisicamente l'utente o per utilizzarle in truffe di ingegneria sociale. Ad esempio, mentre l'utente svolge la sua consueta corsa mattutina, i criminali potrebbero inviare messaggi alla sua lista di contatti tramite un

account falso, sostenendo che la batteria dello smartphone si è scaricata e che ha bisogno di assistenza finanziaria a causa di un "infortunio". È quindi fondamentale prestare attenzione e condividere i propri percorsi solo con persone fidate, evitando di renderli pubblici.

I fitness tracker possono divulgare i dati degli utenti sia intenzionalmente sia involontariamente, spesso amplificando i rischi perché prodotti da aziende soggette a una supervisione normativa minima. In modo intenzionale, alcune società, soprattutto quelle meno conosciute o più economiche, possono monetizzare i dati raccolti condividendoli o vendendoli deliberatamente (spesso in forma anonima o aggregata) a terzi come inserzionisti, broker di dati o persino compagnie di assicurazione. In questo modo, modelli di geolocalizzazione, tendenze della frequenza cardiaca, cicli del sonno e dettagli sulla salute auto-dichiarati diventano una merce redditizia, utilizzabile per attività di marketing mirato senza che gli utenti ne siano pienamente consapevoli. Ciò può incidere anche sui premi dell'assicurazione sanitaria in alcuni mercati e, nei paesi con sistemi sanitari privatizzati, potrebbe comportare costi aggiuntivi.

Può inoltre accadere che, nei dispositivi più economici, prevalgano involontariamente pratiche di sicurezza inadeguate. Una crittografia debole dei dati archiviati nel cloud, vulnerabilità non corrette o negligenza nella protezione dei server possono infatti portare a violazioni in cui gli aggressori accedono, espongono o rivendono enormi set di dati provenienti da dispositivi indossabili sincronizzati.

Con eventi di questa portata che stimolano un aumento dell'entusiasmo per il fitness, gli appassionati devono dare priorità alla sicurezza dei dati rispetto al risparmio. I tracker economici possono diventare porte d'accesso allo sfruttamento. Affidatevi a brand affermati con comprovata esperienza in materia di privacy per evitare che i vostri obiettivi di salute diventino terreno fertile per gli hacker. Tuttavia, anche su questi dispositivi è necessario esaminare attentamente l'informativa sulla privacy e limitare la visibilità dei dati relativi all'allenamento, ha aggiunto Anna Larkina, Web Content and Privacy Analysis Expert di Kaspersky.

Per proteggerti durante l'allenamento o il monitoraggio della salute, Kaspersky consiglia di:

Contatti:
Kaspersky
kaspersky@noesis.net

COMUNICATO STAMPA - CONTENUTO PROMOZIONALE

Responsabilità editoriale di Kaspersky

??

immediapress

Categoria

1. Comunicati

Tag

1. ImmediaPress

Data di creazione

Febbraio 5, 2026

Autore

redazione

default watermark