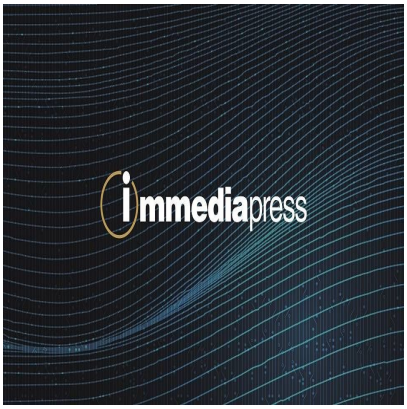

Sport invernali e fitness tracker: lâ??entusiasmo per lâ??attivitÃ fisica puÃ² mettere a rischio i dati personali

Descrizione

default watermark

COMUNICATO STAMPA â?? CONTENUTO PROMOZIONALE

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

Con lâ??inizio dei giochi invernali, milioni di fan in tutto il mondo si sintonizzeranno per vedere gli atleti dâ??Ã©lite 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 allâ??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 piÃ¹ elevati.

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

Tuttavia, la pubblicazione dei dati GPS, sia allâ??interno delle app fitness associate al dispositivo sia sui social network, puÃ² fornire a potenziali aggressori informazioni utili per tracciare fisicamente lâ??utente o per utilizzarle in truffe di ingegneria sociale. Ad esempio, mentre lâ??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 Ã¨ scaricata e che ha bisogno di assistenza finanziaria a causa di un â??infortunioâ?•. Ã? 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 perchÃ© prodotti da aziende soggette a una supervisione normativa minima. In modo intenzionale, alcune societÃ , soprattutto quelle meno conosciute o piÃ¹ 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 attivitÃ di marketing mirato senza che gli utenti ne siano pienamente consapevoli. CiÃ² puÃ² incidere anche sui premi dellâ??assicurazione sanitaria in alcuni mercati e, nei paesi con sistemi sanitari privatizzati, potrebbe comportare costi aggiuntivi.

default watermark

PuÃ² inoltre accadere che, nei dispositivi piÃ¹ economici, prevalgano involontariamente pratiche di sicurezza inadeguate. Una crittografia debole dei dati archiviati nel cloud, vulnerabilitÃ 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.

â??Con eventi di questa portata che stimolano un aumento dellâ??entusiasmo per il fitness, gli appassionati devono dare prioritÃ alla sicurezza dei dati rispetto al risparmio. I tracker economici possono diventare porte dâ??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 Ã¨ necessario esaminare attentamente lâ??informativa sulla privacy e limitare la visibilitÃ dei dati relativi allâ??allenamentoâ?•, ha aggiunto Anna Larkina, Web Content and Privacy Analysis Expert di Kaspersky.

Per proteggerti durante lâ??allenamento o il monitoraggio della salute, Kaspersky consiglia di:

Contatti:
Kaspersky
kaspersky@noesis.net

COMUNICATO STAMPA â?? CONTENUTO PROMOZIONALE

ResponsabilitÃ editoriale di Kaspersky

â??

immediapress

Categoria

1. Comunicati

Tag

1. ImmediaPress

Data di creazione
Febbraio 5, 2026
Autore
redazione

default watermark