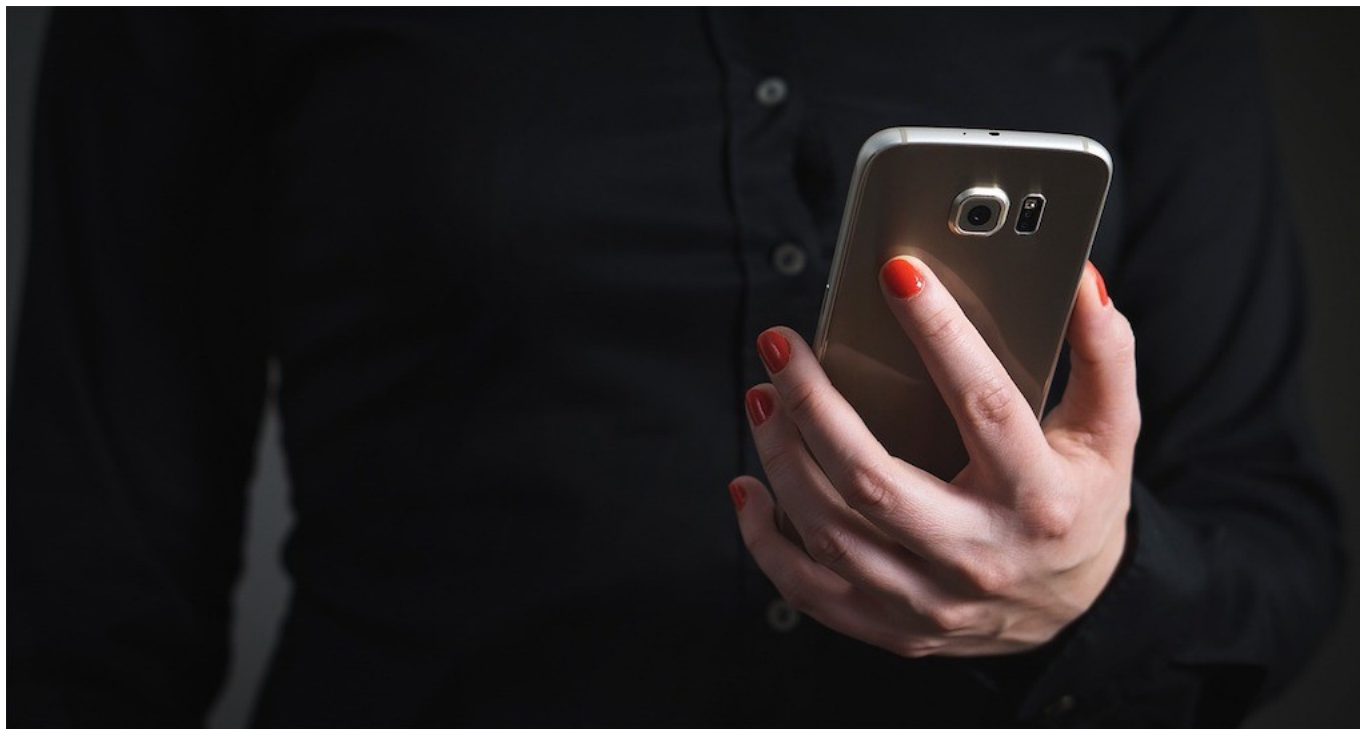


## SICUREZZA E GUSTI MUSICALI: QUANDO CONDIVIDERE PUO' ESSERE PERICOLOSO

6 Marzo 2024



In Italia siamo dei grandi ascoltatori di musica. Che sia pop, rap, rock o di qualsiasi altro genere, molti italiani ascoltano musica sui vari servizi disponibili online, come Spotify, Apple Music, Tidal o Amazon Music. Questi servizi hanno varie offerte, ma alla fine dei conti propongono tutti lo stesso servizio, ovvero quello di rendere disponibile all'ascolto le migliori canzoni dei più quotati artisti musicali del mondo.

Spotify è sicuramente il servizio più apprezzato qui in Italia, e di recente ha superato i 13 milioni di [utenti italiani](#) sulla piattaforma, con artisti italiani che ricevono milioni di ascolti ogni mese.

Come avrete visto dal titolo, però, siamo qui per parlare anche di sicurezza online. Come possono incastrarsi tra di loro questi due argomenti? Il tutto passa da un singolo termine: "condivisione".

Molti utenti, infatti, condividono le canzoni che ascoltano tramite i vari social network (Instagram, Tik Tok e molti altri), ma dietro una semplice condivisione può esserci un pericolo.

In questo articolo approfondiremo questo argomento con dati e consigli per chi vuole proteggersi online.

### L'evento "Spotify Wrapped"

Spotify ha sempre cercato delle idee originali per coinvolgere il suo pubblico, e l'evento a cadenza annuale "Spotify Wrapped" è una di queste. Per chi non lo conoscesse, Spotify Wrapped è un evento che racchiude i gusti e gli ascolti degli utenti di Spotify. Ogni utente riceve un carosello grafico legato alle canzoni, agli artisti e ai suoi generi preferiti, perfino gli stati d'animo legati alle canzoni.

Il Wrapped è stato condiviso nelle storie Instagram di molti utenti, e la maggior parte della gente che ha assistito all'evento ha partecipato a sua volta.

Una parte, però, ha preferito astenersi, poiché alcuni utenti si sono accorti dell'eccessivo tempo speso sulla nota piattaforma di streaming. Gli utenti tra i 35 e i 44 anni ascoltano musica in streaming per più di 28 mila minuti, quasi 20 giorni in totale! Forse per la paura del dato, o magari per la timidezza, questa parte di utenti attivi ha preferito semplicemente visualizzare i dati e restare nella propria "bolla".

Qual è il rischio della condivisione di dati come nel Wrapped?

Purtroppo, l'essere umano può compiere atti sbagliati anche contro la propria volontà, e con l'arrivo dei social network i danni di questi atti si sono amplificati. Molti di noi hanno un idolo, che spesso si rivela essere un artista musicale, e il problema arriva quando il nome di questo artista può essere utilizzato per ciò che dovrebbe essere lo "scudo" dei nostri account, ovvero le nostre credenziali.

[Informazioni](#) come cantante preferito, squadra del cuore o simili sono un vero terreno fertile per i criminali informatici, a cui viene sicuramente facilitato il lavoro tramite queste ingenuità. Ecco perché, soprattutto se questi elementi sono presenti nelle tue password, è sicuramente sbagliato condividere tali informazioni pubblicamente online.

In che modo Spotify "traccia" gli utenti

Al contrario di ciò che si pensa, anche Spotify (come molte delle altre applicazioni famose nei vari store) può tracciare i propri utenti, cosa che si è vista anche nel Wrapped di quest'anno. Tramite un algoritmo appositamente studiato, Spotify è riuscito a tracciare le emozioni dei propri utenti in base alle canzoni ascoltate, per poter proporre sempre nuova musica in base alle emozioni private. Tutto ciò, secondo l'azienda, viene svolto in maniera pulita ed etica, ma può far capire la potenza degli strumenti a disposizione di queste compagnie.

Tutto il discorso del tracciamento è legato anche alle varie campagne pubblicitarie. In base ai comportamenti e ai vari dati (generi, artisti, eccetera) vengono proposte le giuste pubblicità al momento più opportuno, per invogliare l'utente ad acquistare o a interagire con un determinato prodotto.

Tutta questa "macchina da pubblicità" è legata anche al nuovo mercato su cui Spotify ha investito molto, ovvero quello del podcasting, dove le pubblicità sembrano fruttare delle somme non indifferenti.

I dati dei clienti vengono quindi condivisi (secondo la Privacy Policy) con i partner pubblicitari principali, che possono sfruttare i contenuti a loro piacimento.

Come non farsi tracciare

Non sono molti i modi in cui limitare questo tracciamento e questo trattamento dei dati, che viene accettato al momento dell'iscrizione; tuttavia, si può sicuramente fare qualcosa.

Prima di tutto, se non vuoi che gli altri vedano cosa stai ascoltando, entra in modalità "Sessione privata", andando sulle Impostazioni di Spotify dal tuo telefono e attivando l'opzione dedicata. In questo modo, i tuoi ascolti non verranno visualizzati dai tuoi amici e non influiranno su ciò che Spotify ti farà vedere nella "Discover Weekly". Su PC, basta cliccare sulla freccia verso il basso che si trova in alto a destra e cliccare su "Sessione privata".

Da Android e iOS puoi limitare le autorizzazioni concesse proprio a Spotify, come rubrica, fotocamera o microfono. Su PC puoi andare nelle impostazioni (dopo aver cliccato sull'icona del tuo profilo), scorrere fino alla voce "Mostra Impostazioni avanzate" e cliccarci sopra. Una volta fatto ciò, puoi bloccare i cookies dell'app su desktop.

Se non vuoi che le pubblicità siano "su misura" in base ai tuoi gusti, puoi disattivare gli annunci in questione dalle Impostazioni sulla Privacy. Nonostante ciò, riceverai comunque lo stesso numero di pubblicità.

Questi servizi usano le pubblicità come principale fonte di reddito (oltre ai vari abbonamenti), perciò non possono rinunciare a un determinato numero di annunci proposti, ma possono (al massimo) evitare quelli che vengono proposti proprio per un determinato tipo di utente, che pur disattivando l'opzione, riceverà comunque pubblicità di vario genere, e Spotify tratterà ogni ricerca, ascolto, like, etc...

Queste azioni da parte dei servizi di streaming legati alla privacy sono fonte di polemica da anni ormai, specialmente quando

si alzò un gran polverone attorno a Mark Zuckerberg sulle presunte vendite di dati sensibili ad altre aziende (il tutto mirato proprio alle pubblicità). Inoltre, Facebook viene spesso collegato agli account di Spotify, ma i dati collegati a Facebook possono essere cancellati tranquillamente, sempre nelle Impostazioni della privacy.

Puoi anche considerare il fatto di usare un browser che limiti l'utilizzo di cookie di terze parti e utilizzare Spotify da lì. Da iOS è possibile anche limitare il tracciamento delle emozioni tramite le impostazioni di privacy.

#### Come proteggersi online

Come hai appena visto, anche dietro a una condivisione da Spotify può nascondersi un'insidia. In realtà, basta navigare online con un basso livello di sicurezza per essere in pericolo. Seguendo alcuni accorgimenti e affidandoti ai servizi giusti, puoi fare davvero la differenza e migliorare la sicurezza online.

Ecco alcuni consigli da tenere a mente per proteggere i tuoi account e i tuoi dispositivi dai soliti tentativi di phishing, attacchi malware e problemi di vario genere:

- Attiva l'autenticazione a 2 fattori: tramite e-mail o numero di telefono, puoi utilizzare l'autenticazione a 2 fattori e proteggere l'accesso tramite un codice inviato via messaggio. Questa è una delle operazioni di base per proteggere il tuo account.
- Utilizza i dati biometrici: molti servizi offrono la possibilità di accedere al proprio account tramite impronta digitale o attraverso il proprio Face ID. Questa funzione può rivelarsi molto utile, poiché i dati biometrici sono unici nel loro genere e rappresentano un ottimo metodo per accedere al proprio account in maniera sicura.
- Utilizza una VPN: [utilizzare una VPN online](#) è uno dei modi migliori per proteggersi mentre si naviga sul proprio browser. Con una VPN, ovvero una rete privata virtuale, è possibile connettersi al server del proprio paese o di molti altri paesi disponibili, con una connessione veloce e protetta, per navigare senza dover pensare che la sicurezza dei tuoi dispositivi sia in pericolo. Tramite una VPN, generalmente disponibile a prezzi davvero economici rispetto alla qualità del servizio, potrai davvero sentirti al sicuro.
- Controlla la lista degli accessi: vari servizi rendono disponibili le liste degli accessi agli account con data, orario e luogo annessi. Controlla la lista e blocca i dispositivi che hanno effettuato un accesso sospetto!
- Utilizza un gestore delle password: oltre alla VPN, anche un gestore delle password può essere davvero utile. Spesso cambiare la password o ricordare tutte le credenziali stabilite in precedenza può essere seccante, ma con un gestore delle password puoi sincronizzare tutte le tue password e accedere ai vari servizi a cui sei iscritto con un solo clic. Inoltre, puoi produrre password "a prova di hacker", protette da crittografie specializzate.

Queste erano solo alcune istruzioni che puoi seguire per migliorare la tua sicurezza online, ma il consiglio generale che possiamo darti è di stare sempre attento, anche quando condividi qualcosa nelle storie, come una canzone del tuo rapper preferito. Speriamo che questo articolo ti sia piaciuto e sia stato utile, e che tu possa prenderti qualche minuto per migliorare la sicurezza dei tuoi dispositivi. Ricordati che quando si naviga online la sicurezza va messa sempre al primo posto!