La sorveglianza commerciale sul web usa il fingerprinting

- Arturo Di Corinto, 19.12.2019

Hacker's Dictionary. Quando navighiamo in rete la pubblicità ci insegue grazie a una serie di tecniche che permettono di conoscere molte informazioni su di noi

Cosa direste se qualcuno vi seguisse di negozio in negozio durante lo shopping natalizio? E se poi guardasse dentro le buste della spesa e nel portafoglio, fino a sbirciare patente e carta di identità? Probabilmente vi arrabbiereste. Eppure è quello che succede con il *fingerprinting*, una tecnica di tracciamento dei comportamenti online basata sull'analisi dei dati che ci lasciamo dietro quando usiamo web e app. Una volta ci preoccupavamo dei *cookies*, usati per memorizzare le abitudini degli utenti durante la navigazione, ma questo è peggio. In fondo la presenza dei *cookies* è regolata per legge e possiamo distruggerli alla fine di ogni sessione web. Il *fingerprint*, l'impronta digitale, invece è una scatola nera.

L'impronta sfrutta il modo in cui app e siti web comunicano con i nostri dispositivi. Ad esempio, quando navighiamo, il browser fornisce automaticamente ai siti alcune informazioni sull'hardware che stiamo usando. È necessario affinché il sito conosca la risoluzione dello schermo per poter caricare una pagina con le dimensioni corrette. Quando si installa un'app mobile invece, il sistema operativo condivide alcune informazioni sull'hardware con l'app. Anche in questo caso ciò è in parte dovuto al fatto che l'app deve sapere che tipo di telefono utilizziamo per adattarsi alla velocità del processore e alle dimensioni dello schermo.

Ma l'impronta che definisce le caratteristiche del cellulare o del computer, come la risoluzione dello schermo, il sistema operativo e il modello, vengono usate per triangolare queste informazioni e pedinarci mentre navighiamo sul web e usiamo le app sul telefonino. Una volta che sono note abbastanza caratteristiche del dispositivo i dati possono essere assemblati in un profilo utile ad autenticare gli utenti per i servizi bancari ma che l'industria pubblicitaria usa in maniera discutibile per monitorare le nostre attività digitali fino a identificarci in maniera univoca come farebbe un'impronta digitale.

Nonostante questo tipo di tracciamento sia noto da diversi anni se ne parla poco. Eppure tutti i siti web più popolari lo utilizzano per il monitoraggio degli utenti, e non si conosce il numero di app mobili che lo utilizzano. Di certo lo fanno i media online monitorati nel progetto Trackography.

Infatti, date abbastanza informazioni, l'impronta digitale può essere molto affidabile. In uno studio francese, i ricercatori hanno scoperto che circa un terzo delle impronte digitali che avevano raccolto erano uniche e quindi identificabili. In uno studio del 2017, i ricercatori della Lehigh University e della Washington University hanno dimostrato invece che è possibile identificare il 99 percento degli utenti grazie ad essa.

L'impronta digitale infatti raccoglie caratteristiche apparentemente innocue come lingua, browser, sistema operativo e *timezone*, presenza di *cookie* ed estensioni, che sono generalmente condivisi di default per far funzionare correttamente app e siti Web. Anche se navigate in maniera anonima.

Per capirlo si può fare un test con Panopticlik, un progetto della Electronic Frontier Foundation che consente di verificare online quante informazioni su di noi vengono condivise dagli elementi traccianti per il *fingerprinting* e decidere se bloccarle dal browser o con particolari estensioni.

Nel caso delle app invece il consiglio è di eliminare quelle, spesso gratuite, ma poco usate, o di marchi sconosciuti che utilizzano il *fingerprinting*.

Potete anche non farlo, ma la prossima volta che su Amazon vi propongono la felpa blu che vi è tanto piaciuta su Facebook non vi lamentate.