Smartphone e smartwatch, facile arrivare al nostro codice bancomat con il digital profiling

Il termine ***digital profiling*** indica quell'insieme di tecniche e tecnologie utili a isolare ed esaminare nel dettaglio le caratteristiche del comportamento umano. Di solito sono sfruttate per dare la caccia ai cyber criminali, ma purtroppo sempre più spesso sono utili anche agli stessi cyber criminali per monitorare il comportamento degli utenti di rete nell'utilizzo dei loro dispositivi elettronici.

Si tracciano profili psicologici, anagrafici, comportamentali degli autori di un reato come di un semplice cittadino che fa sport all'aperto o altra attività, indossando tecnologie in grado di registrare tutti i nostri parametri vitali sotto sforzo.

Nel nostro caso, le tecniche di *profiling* sono fondamentali per i criminali digitali nel capire in che modo sottrarre informazioni utili sulla nostra vita col fine di farci cadere vittime di azioni illecite, generalmente per sottrarci denaro.

Come il *digital profiling* di un criminale descrive le modalità con cui si compie un reato, consentendo alle forze dell'ordine di risalire all'identità degli autori, così i cyber criminali possono capire dall'uso che facciamo dei nostri device che tipo di persone siamo, cosa facciamo più spesso, quando e perché.

Ad esempio, per mantenere uno stile di vita sano, molti di noi usano i ***fitness tracker*** e ***activity tracker*** per monitorare la propria attività fisica e sportiva, ma anche i parametri vitali di base. Un'abitudine che potrebbe avere anche delle conseguenze pericolose in termini di sicurezza informatica e digitale.

I dispositivi ***wearables*** (tecnologie indossabili), compresi gli ***smartwatch*** e i già citati *fitness tracker*, sono utilizzati di solito nel corso delle attività sportive, per monitorare la nostra salute, ricevere notifiche push e altro ancora. Per svolgere le loro funzioni principali, la maggior parte di questi dispositivi è dotata di sensori di accelerazione incorporati (gli accelerometri), che sono spesso combinati con sensori di rotazione (i giroscopi) per il conteggio dei passi e per conoscere la posizione corrente del loro utilizzatore.

In un esperimento condotto sulla sicurezza dell'internet delle cose, i ricercatori di Kaspersky Lab hanno sviluppato un'applicazione per *smartwatch* abbastanza semplice per registrare segnali da accelerometri e giroscopi integrati. I dati registrati sono stati quindi archiviati nella memoria del dispositivo *wearable* o caricati sullo ***smartphone*** abbinato allo stesso tramite *bluetooth*.

Utilizzando gli algoritmi matematici disponibili per la potenza di calcolo del *wearable*, "*è stato possibile identificare alcuni modelli comportamentali, capire il momento e il luogo nel quale un utente si stava muovendo e anche per quanto tempo ha condotto una certa azione*".

Cosa ancora più importante, "***è stato inoltre possibile identificare alcune attività sensibili degli utenti, compreso l'inserimento di una passphrase sul computer*** *(con una precisione fino al 96%),* ***l'uso di un codice PIN presso i***

bancomat *(circa all'87%) e lo sblocco del proprio smartphone (circa al 64%)".*

Lo stesso set di dati del segnale è un modello comportamentale unico per il proprietario del dispositivo. Utilizzando questo, "*una terza parte (quindi un potenziale cyber criminale) potrebbe andare oltre* ***e cercare di riconoscere l'identità dell'utente, sia tramite un indirizzo email richiesto in fase di registrazione da una app, sia tramite l'accesso alle credenziali dell'account su Android***".

Dopo questo, ci assicurano i ricercatori, "*l'identificazione di informazioni dettagliate su una potenziale vittima – compresa la sua routine quotidiana o i momenti nei quali vengono inseriti dati importanti – è solo una questione di tempo*".

Un esperimento simile è già stato condotto nel 2016 in Danimarca e riportato in un articolo del Sole 24 Ore. Teoricamente e praticamente, rubare il pin del bancomat alle persone dotate di uno smartwatch è possibile. È quanto dimostrato da uno studente dell'Università di Copenhagen, Tony Beltramelli, che ha realizzato per la sua tesi di laurea magistrale un'app per smartwatch in grado di "l*eggere*" i movimenti della mano mentre utilizza una tastiera a 12 tasti, di quelle insomma utilizzate per esempio nei bancomat o anche per lo sblocco dei cellulari.

Come capire se si è vittima di cyber criminali che sfruttano i nostri device indossabili?

Di seguito alcune osservazioni utili: se l'applicazione invia

una richiesta per il recupero delle informazioni sull'account dell'utente, questo potrebbe essere un motivo di preoccupazione, i cybercriminali potrebbero facilmente ricostruire una sorta di "impronta digitale"; la richiesta di permesso per l'invio di dati di geolocalizzazione da parte dell'applicazione dovrebbe essere un motivo di preoccupazione; un consumo veloce della batteria di un dispositivo può essere un ulteriore campanello di allarme.

The post Smartphone e smartwatch, facile arrivare al nostro codice bancomat con il digital profiling appeared first on Key4biz.

https://www.key4biz.it/smartphone-e-smartwatch-facile-arrivare-al-nostro-codice-bancomat-con-il-digital-profiling/222758/