SosTech. I nostri smartphone ci spiano davvero?

Lo scorso maggio, a **Portland**, nell'Oregon, una famiglia ha ricevuto una telefonata piuttosto inconsueta (e allarmante): «*Staccate immediatamente i vostri dispositivi Alexa, c'è un tentativo di hacking ai vostri danni*». In effetti, tutte le stanze della casa erano dotate di **Amazon Echo** per controllare le luci, il riscaldamento, l'allarme – insomma, tutti i sistemi **domotici** che oggi consentono di gestire in remoto, da un'app del proprio smartphone, quasi ogni aspetto della propria abitazione, magari potendo contare anche su un'**assistente vocale** (**Alexa**, appunto) pronto a rispondere alle domande e a trasmettere la musica preferita. L'autore della telefonata era uno dei dipendenti del marito, che sosteneva di aver ricevuto file audio relativi a una conversazione privata della famiglia. «*Impossibile*». «*Stavate parlando di parquet in legno massello*».

Era vero: a 176 miglia di distanza, era arrivata la registrazione audio della loro conversazione, senza che nessuno avesse attivato Alexa. Dunque è vero? I nostri sistemi sempre più sofisticati di intelligenza artificiale ci spiano? Lo stato di "allerta" costante degli apparecchi perennemente collegati alla rete a causa di **offerte Internet** sempre più convenienti (su **SosTariffe.it** potete trovare le migliori del momento) è, oltre che una notevole comodità, anche un rischio?

La spiegazione dell'accaduto si può riassumere con "incredibile serie di coincidenze", e in effetti non si sono verificati altri casi del genere, per cui la possibilità che ricapiti ad altri è infinitesimale. Ma non basta per rimanere

tranquilli. Mentre marito e moglie erano impegnati in una conversazione sull'arredo di casa, uno dei due aveva detto una parola che l'assistente vocale di Amazon – sempre pronto ad attivarsi se interpellato – aveva interpretato come "Alexa". Poi qualcuno aveva parlato di "inviare un messaggio", richiesta (presunta) alla quale l'assistenza aveva risposto "A chi?", scegliendo poi il primo nome plausibile pronunciato il resto della conversazione, chiedendo conferma e pensando di sentire un "sì". Il tutto con i padroni di casa completamente ignari del fatto che il loro assistente vocale stesse iniziando a registrare il messaggio da mandare a uno dei loro contatti.

La privacy? Attenzione anche agli alberghi

L’accaduto sembrerebbe insignificante, ma non in periodo come quello che stiamo vivendo (con i dati di 87 milioni di americani finiti a loro insaputa, com’è noto, in pasto a **Cambridge Analytica**). Non quando è impossibile essere davvero certi che i nostri assistenti virtuali non ci stiano spiando. Immediatamente dopo il fatto di Portland, due senatori USA, **Jeff Flake** (repubblicano) e **Chris Coons** (democratico), hanno chiesto spiegazioni ad **Amazon**: 30 domande, tra cui la richiesta di rendere noti episodi analoghi, la frequenza con cui gli apparecchi come Echo inviano i dati vocali ai server di Amazon, la durata della conservazione di questi dati e le modalità di anonimato garantite dalla società.

Con un tempismo forse non proprio perfetto, qualche giorno dopo Amazon ha lanciato il suo nuovo servizio, **Alexa for Hospitality**, che porta l’assistente digitale anche negli hotel, pensato ad esempio per trasferire al personale (umano o digitale) dell’albergo le richieste degli ospiti di cambiare la temperatura, regolare le luci, trovare consigli sui ristoranti nei paraggi e così via. **Chris Clifton**, professore di Computer Science alla **Purdue University**, ha ricordato che le possibilità che si verifichi nuovamente un caso come quello della famiglia di Portland sono molto limitate, ma ciò non toglie che le ansie per la privacy possano essere addirittura moltiplicate in un contesto come quello di un hotel: basterebbe dimenticarsi di disattivare il proprio account Amazon (fondamentale per poter avere dei consigli personalizzati) prima dell’arrivo di un nuovo ospite per creare tutta una serie di problemi facilmente inimmaginabili.

Lo studio della Northeastern University

Ma per molti la paura non arriva dagli assistenti digitali casalinghi, in Italia ancora non molto diffusi. È lo smartphone, sempre vicino a noi e sempre potenzialmente pronto a rispondere ai nostri "**Ehi, Siri**" e "**Ok, Google**", che potrebbe spiare le nostre conversazioni e usarle per i suoi scopi, carpendo informazioni utili riguardo ai nostri dati più sensibili. Per rispondere a questi dubbi, una serie di studiosi della **Northeastern University** – **Elleen Pan, Jingjing Ren, Martina Lindorfer, Christo Wilson** e **David Choffnes** – hanno passato l'anno scorso a effettuare un esperimento coinvolgendo più di 17.000 delle app più popolari disponibili su Android, per capire se effettivamente qualcuna stesse usando il microfono del dispositivo all'insaputa dell'utente per registrare audio. Fra queste app c'erano ovviamente anche

quelle di Facebook e più di 8.000 che a Facebook inviano informazioni di vario tipo.

Per fortuna non è stata trovata alcuna prova dell'esistenza di un'app in grado di attivare il microfono a tradimento o inviare i file vocali se non richiesta. Ma c'è dell'altro, qualcosa che gli stessi ricercatori non si aspettavano di trovare: la dimostrazione che esistono app che registrano quello che accade sullo schermo dello smartphone e lo inviano a terze parti. Per esempio **GoPuff**, un'app di delivery rivolta specificatamente a chi ha improvvisi desideri di cibo spazzatura, ha registrato l'attività sullo schermo durante l'interazione dell'utente e l'ha spedita ad **Appsee**, una società di analisi. Tra gli screen inviati, anche uno dove era possibile inserire anche dati personali, in particolare il codice fiscale.

Di per sé, il comportamento di Appsee non è del tutto un mistero, visto che la stessa società (a partire dal nome) rivendica fieramente la sua "capacità" di sapere cosa accade sui telefoni degli utenti, ma il problema è che nei casi analizzati dai ricercatori lo faceva senza che fosse evidente agli utenti, e senza che la policy di GoPuff lo segnalasse: contattati dagli autori dello studio, i responsabili di GoPuff sono poi corsi ai ripari, mentre Appsee ha incolpato la startup dell'accaduto. A prescindere dai torti e dai motivi di questa registrazione indebita o perlomeno inattesa (lo scopo di GoPuff era quello di ricavare dati su cui basarsi per migliorare la performance dall'applicazione), il pensiero che il nostro smartphone continui ad essere **u**n compagno non troppo discreto è difficile da cancellare.

Lo stesso studio della Northeastern University d'altronde non

pretende di stabilire che le app utilizzate non ricorrono in nessun caso alle registrazioni senza permesso, visto che l'esperimento è stato effettuato con un programma automatizzato e non con utenti in carne e ossa, che potenzialmente avrebbero potuto interagire con le app in modo diverso, tanto da "attivarle". In più, gli stessi telefoni erano al chiuso in uno sgabuzzino, e non circondati da suoni, rumori e contesti esterni – un po' come la casuale parola "Alexa" sentita da Amazon Echo in una casa di Portland. La paranoia forse è eccessiva, ma un pensierino su ciò che affidiamo ai nostri telefoni è sempre il caso di farlo.

Fonti:

https://www.kiro7.com/news/local/woman-says-her-amazon-device-recorded-private-conversation-sent-it-out-to-random-contact/755507974

https://www.wired.com/story/senators-flake-coons-demand-answers-amazon-echo-privacy/

https://www.purdue.edu/newsroom/releases/2018/Q2/amazon-alexa-devices-in-hotels-raise-privacy-concerns-for-some.html

https://android.jlelse.eu/apple-vs-android-a-comparative-study-2017-c5799a0a1683

The post SosTech. I nostri smartphone ci spiano davvero? appeared first on Key4biz.

https://www.key4biz.it/sostech-i-nostri-smartphone-ci-spiano-davvero/226391/