SMARTPHONE

‘È il prezzo da pagare per avere tecnologie sempre più autonome e intelligenti’

In tanti usano questi dispositivi anche per lavoro e potrebbero insorgere problemi, pure legali, in caso di fughe di dati sensibili DEPOSITPHOTOS

I telefoni ci ascoltano anche senza usarli

di Federica Ciommiento

Sei a cena con amici, parli di quell’auto che vorresti comprare e il giorno dopo ti ritrovi sui social la pubblicità della concessionaria che vende proprio quel modello lì. È una coincidenza o i telefoni davvero ci ascoltano? Nella maggior parte dei casi, per quanto possa non piacerci, la risposta corretta è la seconda. «Spesso siamo proprio noi a dare il consenso alle applicazioni di registrare informazioni audio e video. Per questo è importante essere consapevoli e responsabili», ci spiega **Alessandro Trivilini**, responsabile del Servizio informatica forense della Scuola universitaria della Svizzera italiana (Supsi). Il telefono, però, molti lo usano anche per lavoro e potrebbero insorgere problemi, pure legali, in caso di fughe di dati sensibili.

Gli smartphone possono davvero registrare ciò che diciamo mentre non li stiamo utilizzando?
Prima di tutto bisogna ricordare che lo smartphone è dotato di microfoni e videocamere in grado di captare immagini e suoni anche quando non li stiamo usando. Inoltre siamo nell’epoca degli assistenti vocali come Alexa o Siri. Questi software sono addestrati, grazie all’intelligenza artificiale, a comprendere ciò che vedono e sentono. Gli scopi sono principalmente due: da una parte essere in grado di rispondere sempre meglio alle domande che gli poniamo, dall’altra accrescere la profilazione dell’utente per i vari servizi di marketing. Lo stesso fanno altre applicazioni. È un patto che spesso instauriamo nel momento in cui decidiamo di usare questi strumenti gratuitamente. È il prezzo da pagare per avere tecnologie sempre più autonome e intelligenti.

Li portiamo proprio dappertutto DEPOSITPHOTOS

Spesso si pensa che non sia un problema, che tanto ‘non ho nulla da nascondere’.
Esattamente. Tutti però abbiamo dei momenti privati che vogliamo tutelare, che desideriamo non vengano divulgati all’esterno e che potrebbero compromettere la nostra immagine o la reputazione dell’azienda.

In quale momento diamo il permesso per la registrazione di informazioni video o audio?
Accettando le condizioni di utilizzo che ci vengono proposte quando scarichiamo un’applicazione o dando il consenso per esempio all’utilizzo del microfono o della fotocamera.

Come si può evitare ciò senza rinunciare a scaricare un’app che ci interessa?
Configurando le applicazioni. Nelle impostazioni è possibile scegliere quali funzioni consentire oppure no. Per esempio posso impedire che venga usato il microfono quando l’app non è attiva.
In questo modo gestisco gli strumenti digitali non lasciando che siano sempre in ascolto. Devo però essere consapevole delle conseguenze. Ad esempio limitando la capacità di Siri di captare informazioni, le risposte alle domande che gli pongo saranno probabilmente meno rilevanti rispetto alle mie aspettative.

Posso sapere cosa è stato registrato?
Le applicazioni hanno l’obbligo di indicare nelle condizioni d’uso se raccolgono dei dati e se li registrano. In quest’ultimo caso sono tenute a indicare in quali momenti raccolgono le informazioni, quali memorizzano e con che finalità lo fanno. Questo nel rispetto delle leggi sulla protezione dei dati sempre più presenti anche sul nostro territorio.

Quando attiviamo la modalità ‘in aereo’ il telefono può immagazzinare comunque informazioni da inviare in seguito?
Sì, in quel momento impedisco allo smartphone di interagire col resto del mondo, ma se uso un’app questa potrebbe memorizzare determinati dati, come parti di conversazioni. Per essere sicuri che non venga salvato nulla, il telefono deve essere spento e ancora meglio senza batteria. Cosa non sempre evidente con gli smartphone che ci sono ora.

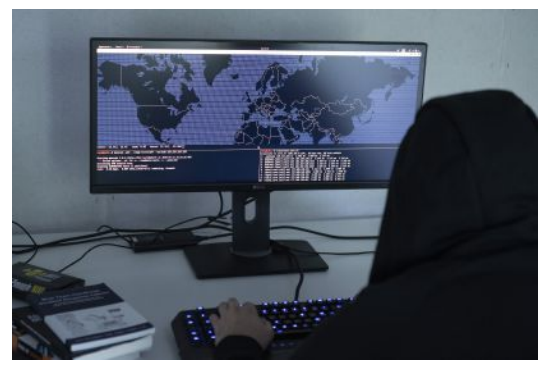
Addirittura senza batteria?
Per esempio nei telefoni è possibile inserire un ‘trojan’, ovvero un tipo di programma controllato a distanza. È in grado di vedere, ascoltare, tracciare quello che faccio senza che me ne accorga. Può funzionare anche a telefono spento e necessita di pochissima batteria. L’accesso remoto e non autorizzato a microfono e videocamera non avviene solo nei film.

Chi inserisce questi programmi negli smartphone? E come lo fa?
L’autorità giudiziaria potrebbe decidere di mettere sotto controllo un telefono per motivi d’inchiesta. Parlando invece di illegalità, a immettere i trojan sono i cosiddetti criminali informatici. I modi per ‘infettare’ i dispositivi sono svariati. Un malware potrebbe essere nascosto nelle applicazioni, nei videogiochi o nei file che scarico da siti fasulli di dubbia provenienza, oppure all’interno di una pagina web che apro. Lo scopo è spesso quello di captare dati sensibili e ricattare la persona, oppure raccogliere informazioni da vendere sul dark web. Consapevolezza e responsabilità sono dunque due elementi fondamentali, perché quando qualcosa del genere succede è difficile risalire al colpevole. Chi delinque sfrutta al massimo la territorialità e le leggi diverse dei Paesi. Raramente l’autore si trova fisicamente vicino a noi, la criminalità informatica non ha confini. Inoltre nel dark web la regola è che non ci sono regole.

Le leggi sono tanto diverse tra i vari Paesi?
C’è la tendenza a uniformare l’approccio alla sicurezza, ad avere strumenti interoperabili tra Paese e Paese: di tipo giuridico, tecnico e di intervento. Questo proprio perché di fronte alla volatilità di queste tecnologie e situazioni è necessario avere punti in comune di azione e tutela.

È possibile chiedere che i dati registrati vengano cancellati?
Sulla base del diritto all’oblio è possibile richiederne l’eliminazione. Questo se i dati non sono stati recuperati in modo trasparente o non proporzionato con le finalità per cui sono stati raccolti. È però una regola che nella realtà non trova sempre riscontro. I colossi generalmente non sono molto reattivi e non hanno nemmeno l’interesse a togliere dati se non si tratta di qualcosa come una violazione dell’integrità della persona, una violenza, un omicidio o un fatto grave. In ogni caso una tutela legale esiste, ma ricordiamoci che nello scenario della criminalità e del dark web le regole diventano molto fragili.

Gli smartphone vengono spesso usati per lavoro, quindi ci possono essere anche rischi per le aziende.
Se la criminalità informatica ha nel mirino una ditta, spesso colpisce prima i telefoni dei vari manager per raccogliere notizie necessarie per preparare il vero e proprio attacco informatico all’azienda. Ricordiamoci però che nessuno è esente da crimini di questo genere. Pensiamo al revenge porn: le persone vengono registrate in momenti intimi e poi ricattate. Questo succede e noi vediamo vari casi anche in Ticino. Analizzando l’accaduto spesso si scopre che la vittima ha scaricato dei giochi, oppure preso parte a community o blog non sicuri ma emotivamente molto attrattivi.



La criminalità informatica non ha confini KEYSTONE

È anche vero che non sempre i datori di lavoro forniscono un dispositivo e quindi si finisce per avere vita privata e professionale in un posto solo.
Il mondo del lavoro sta cambiando e l’intersezione fra vita privata e professionale può creare delle porte d’accesso che vengono sfruttate dalla criminalità informatica e non solo. Quando usiamo il telefono per scopi personali abbiamo la tendenza ad abbassare la guardia, installando applicazioni ricreative o acconsentendo ai software l’accesso a determinate funzioni. Alla sicurezza si fa anche meno attenzione quando si sta lavorando e si è di fretta.

Un’azienda come può proteggersi?
Ci sono tre assi che garantiscono, se presenti insieme, un buon grado di sicurezza. Il primo è quello di fornire ai dipendenti un’alfabetizzazione digitale costante, in cui si mostra cosa potrebbe succedere e come comportarsi. In secondo luogo è importante avere delle linee guida per l’utilizzo degli strumenti digitali a scopo professionale. Queste devono essere aggiornate alle modalità di lavoro ibride che portano spesso a lavorare fuori dal perimetro aziendale. Il terzo punto è scegliere i dispositivi più consoni in funzione degli obiettivi della ditta e delle attività che il dipendente svolge, dotandoli di tutti i crismi di sicurezza necessari.