Ministero dell'Istruzione, dell'Università e della Ricerca
ISTITUTO COMPRENSIVO STATALE
Piazza della Repubblica 6 - 10083 FAVRIA tel. 0124 470067
e-mail: TOIC865006@istruzione.it - sito web:www.icfavria.edu.it
C.F. 85502080014 – C.M. TOIC865006

Al personale

Alle famiglie

IC Favria

Favria, 5.11.2021

Si rendono note indicazioni a tutela della riservatezza dei dati attraverso un articolo di L.Gamalero del Team GDPR Scuola che collabora con l'Istituzione scolastica

Si invita ad attenta lettura

F.to Il Dirigente Scolastico

Dott.ssa Valeria MIOTTI

Firma autografa sostituita a mezzo stampa

ai sensi dell'art. 3 comma 2 del D.L. 39/93

Come i microfoni degli smartphone possono carpire "illecitamente" informazioni personali

di Lucia Gamalero

Privacy Specialist
Responsabile GDPR Scuola

Smartphone e tablet sono strumenti tecnologici ormai ampiamente diffusi in tutte le fasce di età, e soprattutto fra i più giovani.

Se da un lato la tecnologia è da sempre sinonimo di progresso ed evoluzione, è altrettanto vero che un **utilizzo improprio e scarsamente consapevole delle applicazioni installate sui vari device può comportare non pochi rischi**, spesso legati al furto di dati personali e a fenomeni quali l'adescamento online o il cyberbullismo.

Ultimamente una delle minacce principali per la privacy **è rappresentata da tutte quelle app che fanno uso del microfono integrato nello smartphone per raccogliere informazioni poi rivendute illecitamente a società che effettuano proposte commerciali.**

Non è cosa rara, infatti, ritrovare sul proprio telefono messaggi pubblicitari – spesso sotto forma di spam via email – riguardanti prodotti o servizi strettamente correlati ad argomenti di cui si è parlato a voce alta solo pochi giorni prima.

E sebbene quando si installa una nuova applicazione a volte sia necessario prestare il consenso all'utilizzo del microfono, molte app spesso richiedono l'autorizzazione ponendola come un obbligo, pena l'impossibilità di utilizzare il programma.

Tuttavia è piuttosto frequente che si accetti di buon grado la cosa, senza pensarci troppo e senza prendere in esame tutte le possibili complicazioni del caso.

Le indagini da parte del Garante della Privacy

Al fine di arginare il fenomeno e limitare i rischi ad esso correlati, l'Autorità Garante ha avviato un'istruttoria in collaborazione con il Nucleo speciale privacy e frodi tecnologiche della Guardia di Finanza, che prevede l'analisi approfondita di una serie di applicazioni per smartphone tra le più scaricate, verificando altresì che l'informativa resa agli utenti sia realmente chiara e trasparente, e che sia stato correttamente acquisito il relativo consenso.

La nuova attività promossa dal Garante della Privacy va ad affiancarsi a quella già avviata relativa alla semplificazione delle informative mediante simboli ed immagini, al fine di permettere a utenti e consumatori di risultare agevolati nel compiere scelte libere e consapevoli dopo essere stati informati in maniera sintetica, chiara, esaustiva ed efficace.

Come verificare se sullo smartphone sono presenti applicazioni a rischio

Le più recenti innovazioni legate al sistema operativo Android consentono di controllare con facilità quali applicazioni installate sul proprio smartphone sono autorizzate all'utilizzo del microfono.

Per verificare questo elenco è sufficiente ricercare all'interno delle impostazioni la voce relativa alle app, entrare nella parte di gestione, e quindi controllare i permessi relativi all'uso del microfono.

Qualora si noti la presenza di app non autorizzate volontariamente e consapevolmente, è possibile selezionarle per modificare l'autorizzazione.

Se tuttavia l'accesso al microfono è un requisito fondamentale per l'esecuzione dell'applicazione, quest'ultima, durante il primo avvio che segue il download, ne richiederà l'autorizzazione d'uso.

Procedura del tutto simile è prevista anche per il sistema iOS: una volta raggiunta l'apposita sezione, è sufficiente effettuare un "tap" sulla voce "Microfono" per visualizzare la lista delle app che possono utilizzarlo.

Discorso analogo per la fotocamera, mentre altrettanto utile può essere controllare al contempo le app che possono accedere alla posizione mediante i servizi di geolocalizzazione.

Come difendersi dal furto di dati personali da parte degli smartphone

Nonostante la potenziale entità del problema, cedere agli allarmismi ha comunque poco senso.

Numerose applicazioni, quali banalmente quelle per monitorare le videocamere di sorveglianza e quelle di messaggistica istantanea come “WhatsApp” e “Messenger”, non compaiono infatti tra i programmi che raccolgono informazioni al fine di rivenderle per scopi promozionali/commerciali.

Ma se su queste ultime il Garante della Privacy ha già messo in atto tutte le opportune verifiche, occorre in ogni caso prestare attenzione a tutte quelle app ambigue che magari contengono pubblicità o che invitano ad effettuare ulteriori download successivi, quali giochi gratuiti o poco popolari.

Occorre in ultimo puntualizzare come spesso le stesse applicazioni che raccolgono informazioni per poi rivenderle a società terze per effettuare proposte commerciali esplicitino chiaramente di svolgere tale attività all’interno della propria informativa privacy.

È perciò necessario leggere sempre per intero (e con estrema attenzione) quanto proposto, senza trascurare clausole e condizioni spesso accettate ad occhi chiusi, senza pensarci troppo.

L’uso della tecnologia comporta da sempre, oltre a numerosi vantaggi, anche alcuni rischi: se è vero infatti che molte delle conseguenze sono inevitabili, è altrettanto vero che prestando attenzione nel selezionare le applicazioni da scaricare sui dispositivi si può ridurre di parecchio il rischio di subire il furto di informazioni riservate.