La privacy non va mai in vacanza. E-state in privacy, il Vademecum del Garante Privacy sull'utilizzo sicuro dei social network in vacanza

06-08-2018

A distanza di pochi mesi dall'applicazione del Regolamento europeo in materia di privacy tornano utili alcuni consigli pubblicati dal Garante per la Protezione dei Dati Personali sull'utilizzo sicuro dei social network mentre si è in vacanza.

Il Vademecum, *"E-state in privacy. Informazioni utili su selfie e foto, protezione di smartphone e tablet, acquisti on line, uso di app, chat e social network quando si è in vacanza – Edizione 2018"* – pubblicato sul sito https://www.garanteprivacy.it/estate a luglio 2018 – elenca 13 semplici regole ed informazioni per tutelare la privacy anche sotto l'ombrellone.

Di seguito le informazioni utili per tutelare la propria privacy e non violare quella altrui.

Non esagerare con selfie e foto, in quanto non tutti vogliono apparire online durante le vacanze o far sapere a tutto il mondo di internet dove si trova e con chi sta trascorrendo il proprio periodo di ferie. Dunque si consiglia sempre di postare foto previo consenso di tutti i soggetti presenti nella foto stessa, a prescindere dal tag o meno. Inoltre, si raccomanda di evitare di postare foto e video in cui è presente un minore, in quanto dai social network ogni foto e video può essere facilmente scaricata nel pc di qualsivoglia malintenzionato, per cui prima di postare immagini di minori – secondo il Garante – sarebbe utile utilizzare alcune accortezze (es. "pixellare" i volti tramite programmi di grafica, oppure semplicemente posizionando una emoticon sul volto o ancora limitare le impostazioni di visibilità delle foto solo alle persone fidate).
Geolocalizzazione, si o no? Per chi non vuole far sapere dove sta trascorrendo le proprie vacanze estive si suggerisce di disattivare la geolocalizzazione di smartphone e tablet.
I cosiddetti "social-ladri". Secondo il Garante, postando costantemente informazioni sulle nostre vacanze v'è l'elevato rischio che eventuali ladri di appartamento vengano a conoscenza della possibilità di accedere con facilità nella vostra casa "vuota". Il pericolo aumenterebbe notevolmente se poi si danno informazioni sul giorno della partenza e su

quello del ritorno, dando così modo ai "social-ladri" di organizzare senza troppi intoppi il furto del vostro appartamento. In generale, poi, il suggerimento è quello di evitare di diffondere online informazioni personali, quali l'indirizzo o le foto di casa.
Sistemi domotici in casa (videosorveglianza, sicurezza, ecc.). In tali casi il Garante raccomanda di assicurarsi che tali dispositivi siano protetti, mediante password sicure ed aggiornamento costante del software in quanto al pari di tutte le tecnologie connesse online, tali sistemi di sicurezza delle abitazioni possono essere esposti ad attacchi informatici, virus e malware. In particolare, prima di partire si consiglia di spegnere o disconnettere i dispositivi smart che non è necessario lasciare attivi; mentre, per quelli che restano operativi, si consiglia di impostare sistemi di alert per controllarne a distanza il funzionamento e, al contempo, monitorare anche la propria abitazione.

Privacy in valigia. Secondo le raccomandazioni del Garante, anche in vacanza è bene sempre controllare le impostazioni privacy dei vari social network utilizzati, in particolare: a) limitando la visibilità e la condivisione dei post solo agli amici; b) attivare particolari misure di sicurezza come ad esempio il controllo degli accessi al proprio profilo social o un codice di sicurezza che viene inviato via sms o e-mail nel caso si acceda ai social da dispositivi diversi da quelli abituali. Con tali piccole procedure è possibile accorgersi in tempo reale di eventuali accessi abusivi o furti di identità. Infatti, capita spesso, durante i viaggi, di utilizzare i social network su pc di un Internet cafè o su una postazione web messa a disposizione dell'albergo. Dunque, in questi casi, è importante – una volta terminato l'utilizzo del dispositivo – di "uscire" dagli account, rimuovendo così ogni impostazione del browser di navigazione che possa salvare le proprie credenziali.
Attenzione ai "pacchi". Si tratta di eventuali messaggi che contengono offerte su viaggi o affitti di case vacanze, apparentemente convenienti, che invitano a cliccare su un determinato link e che richiedono dati personali o bancari. Con tale tipo di navigazione, virus informatici, software spia, ransomware e phishing possono sempre essere in agguato – sostiene il Garante. Si raccomanda, dunque, di utilizzare servizi online di prenotazione viaggi, hotel, automobili a noleggio, mediante carte di credito prepagate o di altri metodi di pagamento che evitino la condivisione di dati del proprio conto bancario o della carta di credito. Sarebbe utile anche impostare sistemi di alert che avvisano in tempo reale delle transazioni che avvengono sul conto o sulla carta di credito, per accorgersi di eventuali addebiti non autorizzati e, in caso di spiacevoli sorpresi, rivolgersi subito alla propria banca. Buona prassi, infine, è quella di controllare sempre che l'indirizzo dei siti su cui autorizziamo pagamenti online non siano "anomali" (es. verificare che l'indirizzo del sito corrisponde al nome dell'azienda che dovrebbe gestirlo) e se sono

rispettate le procedure di sicurezza per i pagamenti online (URL che inizia con "https" con il simbolo del lucchetto).

App-prova di estate. Molti utenti di smartphone e tablet in vacanza scaricano film , app per giochi, suggerimenti per location turistiche, ecc. Anche questi prodotti possono nascondere virus, pertanto, si raccomanda di: a) scaricare le app dai market ufficiali; b) leggere con attenzione le descrizioni delle app (es., se sono denunciati errori, imprecisioni, ecc.); c) consultare le recensioni degli altri utenti per conoscere eventuali problemi di sicurezza dei dati; d) evitare che i minori possano scaricare film, app o altri prodotti informatici da soli, limitando l'uso sul loro smartphone o creando profili con impostazioni d'uso limitate se usano quello dei genitori.
Per chi non può vivere senza wi-fi. In questo caso, se si usano le connessioni gratuite offerte da bar, ristoranti, stabilimenti balneari ed hotel e non si è certi del grado di sicurezza impostati per proteggere il sistema wi-fi da virus sarebbe meglio evitare di accedere sotto copertura di tali wi-fi a servizi online che richiedono credenziali di accesso (mail, social network, ecc.) o fare acquisti online con la carta di credito o, ancora, anche consultare il conto bancario online.
Protezione alta per non rimanere "scottati". Aggiornmenti software costanti e programmi antivirus dotati di anti-spyware e anti-spam per evitare furti di dati o violazioni della privacy.
Smartphone e tablet pronti a "partire". Può purtroppo accadere di smarrire smartphone e tablet durante le vacanze. Per evitare furti di identità e violazioni della privacy, dunque, è sempre opportuno non conservare dati troppo personali sui device (password e codici bancari) ed evitare che i browser e le app memorizzino le credenziali di accesso a siti e servizi (e-banking, mail, social). Conviene, poi, impostare un codice di accesso sicuro e conservare con cura il codice IMEI, che si trova sulla scatola del dispositivo al momento dell'acquisto che serve e "bloccare" il dispositivo anche a distanza, perlomeno per evitare una violazione della propria privacy.Buona prassi, infine, sarebbe quella di fare un backup di tutte le informazioni presenti sul dispositivo prima di partire (numeri di telefono, foto, ecc.).

Per navigare tranquilli nel mare dei messaggi. Nel periodo estivo si utilizzano spesso sms e chat ma alcuni messaggi potrebbero contenere virus o malware. Secondo il Garante, dunque, è sempre importante fare attenzione a quali programmi scaricare o ad aprire eventuali allegati o cliccare su link che possono essere contenuti nel testo o nelle immagini presenti all'interno del messaggio ricevuto. Alcune precauzioni: a) non rispondere a messaggi provenienti da sconosciuti; b) se si usa un pc è possibile posizione

il mouse sul link "senza cliccare" e verificare – in basso a sinistra nel browser – la URL reale al quali si è indirizzati.

Drone in vacanza. Per gli appassionati di droni a fini ricreativi, muniti di fotocamera su una spiaggia o in altro abituale luogo di vacanza, è buona prassi evitare di invadere gli spazi personali e l'intimità delle persone, di diffondere foto e riprese realizzate con il drone sul web o sui social o in chat che potrà avvenire solo con il consenso di tutti gli interessati, salvi casi particolari di libera manifestazione del pensiero e per fini giornalistici. Nei casi in cui risulta, invece, decisamente difficile raccogliere i consensi di tutti gli interessati, è possibile diffondere immagini e riprese solo se i soggetti non sono riconoscibili, perché ripresi da lontano, o perché ci si affida a dispositivi software che oscuramento volto. Non si possono diffondere immagini di autovetture con targhe visibili (a meno che non oscurate) o le riprese che violano gli spazi altrui (es. casa vacanze, camere d'albergo) perché si potrebbe violare l'altrui riservatezza, andando incontro anche a violazione di norme penali. Non si possono, infine, utilizzare droni per captare e diffondere conversazioni altrui.

Non lasciare a casa il buon senso. Infine, il Garante raccomanda tutti ad un uso consapevole ed attento delle nuove tecnologie per una gestione accorta dei nostri dati personali, ricordando ed attuando queste semplici regole.

Il Garante informa, infine, che per maggiori informazioni, è possibile consultare anche la sezione Diritti del sito web www.garanteprivacy.it e lecampagne di comunicazione del Garante.

E´ inoltre possibile rivolgersi per informazioni, chiarimenti o segnalazioni all´Ufficio Relazioni con il Pubblico (URP) del Garante.

di *Noemi Prisco*

La privacy non va mai in vacanza. E-state in privacy, il Vademecum del Garante Privacy sull’utilizzo sicuro dei social network in vacanza

06-08-2018