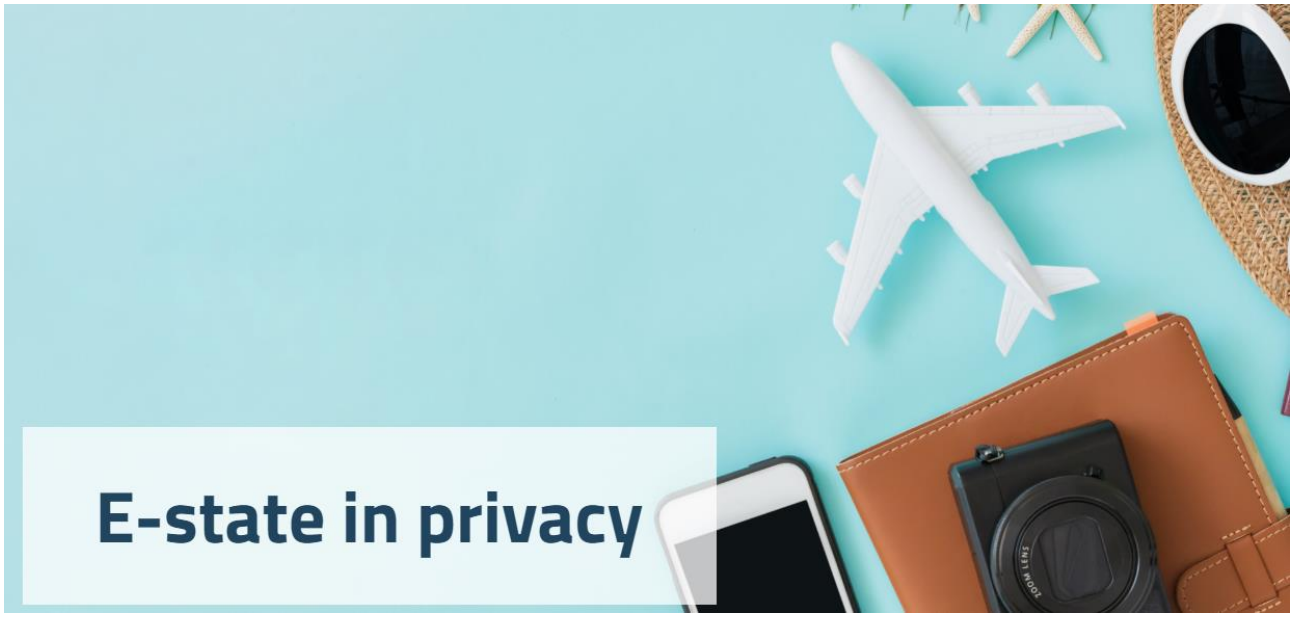

GPDP | GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

E-state in privacy

GPDP 2021

Certifico Srl - IT

ID 14348 | 20.08.2021

E-state in privacy | G-PDP 2021

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 (e non solo)

1. Sotto il sole estivo, non esporti troppo con selfie e foto: protezione alta soprattutto per i minori.

Non tutti vogliono apparire on line, essere riconosciuti o far sapere dove e con chi si trovano durante le ferie estive. Se si postano foto o video in cui compaiono altre persone, è sempre meglio prima accertarsi che queste siano d'accordo, specie se si inseriscono poi anche dei tag con nomi e cognomi.

E' abitudine diffusa condividere foto e video dei propri figli. E' bene essere sempre consapevoli che le immagini dei minori pubblicate on line possono finire anche nelle mani di malintenzionati: meglio quindi evitare di "postarle", oppure almeno utilizzare alcune accortezze, come rendere irriconoscibile il viso del minore (ad esempio, utilizzando programmi di grafica per "pixellare" i volti, semplici da usare e disponibili anche gratuitamente online, o posizionando semplicemente sopra una "faccina" emoticon), oppure limitare le impostazioni di visibilità delle immagini solo alle persone fidate.

2. Geolocalizzati anche in ferie? Per gli amanti della riservatezza che non vogliono far sapere dove sono durante le vacanze estive, il suggerimento è disattivare le opzioni di geolocalizzazione di smartphone e tablet (se non indispensabili per specifici servizi), oltre a quelle dei social network utilizzati.

3. I "social-ladri" non vanno in vacanza. Postando sui social network informazioni sulle vacanze si potrebbe far sapere ad eventuali malintenzionati che la propria casa è vuota.

Il pericolo aumenta se poi si scrive anche quando si parte e per quanto tempo si resterà in ferie.

Il suggerimento è innanzitutto quello di evitare di diffondere on line informazioni molto personali, come ad esempio l'indirizzo di casa o le foto del proprio appartamento.

4. Non "abbandonare" la tua casa. Se sono presenti in casa prodotti e sistemi domotici, è importante ricordare che questi utili dispositivi - al pari di tutte le tecnologie connesse online - possono essere esposti ad attacchi informatici, virus e malware.

Laddove possibile, è quindi bene assicurarsi che siano protetti, ad esempio impostando password sicure e aggiornando costantemente il software pergarantireuna maggiore protezione.

Prima di partire si può decidere di spegnere o disconnettere i dispositivi smart che non è strettamente necessario restino attivi. Per quelli che restano operativi, si possono eventualmente impostare sistemi di alert per controllare anche a distanza il loro funzionamento e magari monitorare anche lo stato della casa.

5. Metti anche la privacy in valigia. Anche in vacanza, è bene controllare le impostazioni privacy dei social network utilizzati, limitando magari la visibilità e la condivisione dei post ai soli amici. Altra buona regola è fare attenzione a non accettare sconosciuti nella cerchia di amicizie on line.

In generale, se disponibili, è bene attivare particolari misure di sicurezza come, ad esempio, il controllo degli accessi al proprio profilo social o un codice di sicurezza da ricevere via sms o e-mail nel caso si acceda ai social network da dispositivi diversi da quelli abituali. In questo modo è possibile accorgersi in tempo di eventuali accessi abusivi alle proprie pagine social personali e di furti di identità.

Durante un viaggio può capitare di utilizzare il pc di un Internet café o una postazione web messa a disposizione dall'albergo per controllare l'e-mail personale o i propri profili social. E' importante in questi casi ricordare - una volta terminata la consultazione - di "uscire" dagli account, rimuovendo così ogni impostazione che consenta di salvare le proprie credenziali nei browser di navigazione.

6. Attenzione ai "pacchi". E´ bene fare attenzione a eventuali messaggi che contengono offerte straordinarie riguardo viaggi e affitti di case per le vacanze da ottenere, ad esempio, cliccando su link che richiedono dati personali o bancari. Virus informatici, software spia, ransomware e phishing possono essere in agguato.

In generale, se si utilizzano servizi online per prenotare hotel, viaggi aerei, automobili a noleggio, ecc., è più prudente usare carte di credito prepagate o altri sistemi di pagamento che permettono di evitare la condivisione di dati del conto bancario o della carta di credito.

E' inoltre utile 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, nel caso, rivolgersi subito alla propria banca o al gestore delle carte.

Altra accortezze utili possono essere quelle di controllare che l'indirizzo internet dei siti su cui si fanno pagamenti on line non appaia anomalo (ad esempio, verificare se non corrisponde al nome dell'azienda che dovrebbe gestirlo) e se vengono rispettate le procedure di sicurezza standard per i pagamenti on line (ad esempio, la URL - cioè l'indirizzo - del sito deve iniziare con "https" e avere il simbolo di un lucchetto).

7. App-prova di estate.

In vacanza molti utenti di smartphone e tablet scaricano film, app per giochi, suggerimenti turistici, ecc.. Questi prodotti possono anche nascondere virus o malware (cioè, software pericolosi).

Per proteggersi, si possono mettere in pratica alcune precauzioni di base:

- scaricare le app dai market ufficiali;

- leggere con attenzione le descrizioni delle app (se, ad esempio, nei testi sono presenti errori e imprecisioni, c'è da sospettare);

- consultare eventuali recensioni degli altri utenti per verificare se sono segnalati problemi di sicurezza dei dati nell'uso di una determinata app, di una piattaforma per il download di film, di un sito, ecc.;

- evitare che i minori possano scaricare film, app o altri prodotti informatici da soli, magari impostando limitazioni d'uso sul loro smartphone o creando profili con impostazioni d'uso limitate se usano quello dei genitori.

8. Per chi non può proprio vivere senza wi-fi. Se si usano le connessioni offerte da bar, ristoranti, stabilimenti balneari e hotel e non si è certi degli standard di sicurezza impostati per proteggere il wi-fi da virus e rischi di intrusione, meglio adottare alcune accortezze, come evitare di accederea servizi online che richiedono credenziali di accesso (ad esempio, alla propria webmail, ai social network, ecc.), fare acquisti on line con la carta di credito oppure utilizzare il conto bancario on line.

9. Scegliere una protezione alta per non rimanere "scottati". Aggiornamenti software costanti e programmi antivirus, magari dotati anche di anti-spyware e anti-spam, possono essere buone precauzioni per evitare furti di dati o violazioni della privacy.

E´ bene mantenere aggiornati anche i sistemi operativi di tutti i dispositivi utilizzati per garantirsi una maggiore protezione.

10. Smartphone e tablet pronti a "partire". Durante le vacanze, può purtroppo accadere che smartphone e tablet siano smarriti o vengano rubati: è quindi bene seguire alcune accortezze.

In generale, è opportuno non conservare dati troppo personali sui device (ad esempio, password o codici bancari) e prendere altre piccole precauzioni, come quella di evitare che i browser e le app memorizzino le credenziali di accesso a siti e servizi (ad esempio, posta elettronica, social network, e-banking).

Per proteggere i dati contenuti nei dispositivi, conviene impostare un codice di accesso sicuro e conservare con cura il codice IMEI, che si trova sulla scatola al momento dell´acquisto e che serve a bloccare il dispositivo a distanza.

Prima di partire potrebbe inoltre essere utile fare un backup di tutte le informazioni (numeri di telefoni, foto, ecc.).

11. Per navigare tranquilli nel mare dei messaggi. Nel periodo estivo si utilizzano molto sms, chat e sistemi di messaggistica. Alcuni messaggi potrebbero però contenere virus, malware o esporre al rischio di spam. E´ quindi sempre bene fare molta attenzione prima di scaricare programmi, aprire eventuali allegati o cliccare su link che possono essere contenuti nel testo o nelle immagini presenti all´interno dei messaggi ricevuti.

Si possono poi adottare semplici precauzioni: ad esempio, non rispondere a messaggi provenienti da sconosciuti. Se si usa un pc, si può passare il mouse su un link senza cliccarlo e verificare - in basso a sinistra nel browser - la URL reale al quale si è indirizzati.

12. Per chi porta il drone in vacanza.

Se si fa volare a fini ricreativi un drone munito di fotocamera su una spiaggia o in un altro abituale luogo di vacanza, è meglio evitare di invadere gli spazi personali e l'intimità delle persone.

La diffusione di riprese realizzate con il drone (sul web, sui social media, in chat) può avvenire solo con il consenso dei soggetti ripresi, fatti salvi particolari usi connessi alla libera manifestazione del pensiero, come quelli a fini giornalistici. Negli altri casi, quando è eccessivamente difficile raccogliere il consenso degli interessati, è possibile diffondere le immagini SOLO se i soggetti ripresi non sono riconoscibili, o perché ripresi da lontano, o perché si sono utilizzati appositi software per oscurare i loro volti. Va in ogni caso utilizzata la massima attenzione nel caso di immagini che ritraggono minori (vedi anche il vademecum "Minori e nuove tecnologie").

Occorre poi evitare di riprendere e diffondere immagini che contengono dati personali come targhe di macchine, ecc. Le riprese che violano gli spazi privati altrui (es: la casa delle vacanze, la camera d'albergo, ecc.) sono invece sempre da evitare, anche perché si potrebbero violare norme penali. Non si possono usare droni per captare volontariamente conversazioni altrui.

13. Non lasciare a casa il buon senso. La miglior difesa anche nel periodo delle vacanze è usare con consapevolezza e attenzione le nuove tecnologie e gestire con accortezza i nostri dati personali, ricordando semplici regole che tutti possono mettere in campo.

Per maggiori informazioni, è possibile consultare anche la sezione Diritti del sito web www.garanteprivacy.it e le campagne di comunicazione del Garante.

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

Fonti:
GPDP

Collegati
GPDP

Matrice Revisioni

Rev.	Data	Oggetto
0.0	20.08.2021	---

Note Documento e legali

ID 14348 | 20.08.2021
Permalink: https://www.certifico.com/id/14348
Policy