GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

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

1. Nella stagione calda, non esporsi troppo con selfie e foto. Non tutti vogliono apparire on line, essere riconosciuti o far sapere dove e con chi si trovano durante le ferie estive. Soprattutto se le immagini possono risultare in qualche modo imbarazzanti. Se si postano foto o video in cui compaiono altre persone, è sempre meglio accertarsi prima che queste siano d'accordo, specie se si inseriscono anche dei tag con nomi e

cognomi. E' bene porre particolare attenzione alle foto di minori, per garantire anche il loro diritto alla riservatezza e proteggerli dall'eccessiva esposizione: le immagini pubblicate on line possono infatti finire anche nelle mani di malintenzionati.

2. Geolocalizzati? No, grazie. 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, oltre a quelle dei social network utilizzati.

3. I "social-ladri" non vanno mai 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 per quanto tempo si resterà in ferie o in quali giorni. Il suggerimento è innanzitutto quello di evitare di postare sul web informazioni troppo personali, come ad esempio l'indirizzo di casa o le foto del proprio appartamento.

4. Non dimenticare di mettere la privacy in valigia. E' bene controllare le impostazioni privacy dei social network utilizzati, limitando 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 device 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 fare sempre il logoff dagli account ed evitare di salvare le proprie credenziali nei browser di navigazione.

5. 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, ramsonware e phishing possono essere in agguato. In generale, se si acquistano servizi - ad esempio 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. Altra accortezza importante è controllare che l'indirizzo internet del sito 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).

6. App-prova di estate. In vacanza molti utenti di smartphone e tablet scaricano app per giochi, suggerimenti turistici, ecc.. Questi prodotti possono anche nascondere virus o malware (cioè, software pericolosi). Per proteggersi, buone regole sono: 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; evitare che i minori possano scaricare app da soli.

7. Per chi non può proprio vivere senza wi-fi. Le connessioni offerte da bar, ristoranti, stabilimenti balneari e hotel potrebbero non essere sufficientemente protette e mettere pc, smartphone e tablet a rischio di intrusioni esterne da parte di malintenzionati a caccia di dati personali. Inoltre, connessioni "infettate" potrebbero veicolare virus e malware, esponendo i dispositivi collegati a diversi rischi, dal phishing al furto di identità. In ogni caso, quando non si è certi del livello di sicurezza della connessione wi-fi, meglio evitare di usare servizi che richiedono credenziali di accesso (ad esempio, alla propria webmail, ai social network, ecc.), fare acquisti on line con la carta di credito o utilizzare il conto on line. Una buona precauzione è disabilitare la funzione di accesso automatico dello smartphone e del pc alle reti wi-fi per poter eventualmente verificare - prima di usarle - se le reti disponibili offrono adeguati standard di sicurezza.

8. 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.

9. Smartphone e tablet pronti a "partire". Durante le vacanze, può 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.) su "chiavette" o hard disk esterni, oppure trasferirle sul cloud. Ovviamente, in quest'ultimo caso, è bene informarsi sulle condizioni contrattuali e sulle garanzie privacy del servizio.

10. 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.

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 e Prevenzione 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.

Roma, 12 luglio 2017