



## Consigli per navigare sicuri durante le vacanze estive

**1. Selfie e dintorni.** Pubblicare le foto o i video delle vacanze sui *social network* è divertente. Ma non tutti vogliono apparire on-line, essere riconosciuti o far sapere dove e con chi si trovavano durante le ferie. Soprattutto se le immagini possono risultare in qualche modo imbarazzanti. Se si postano foto o video con altre persone, è sempre meglio prima accertarsi che queste siano d'accordo, specie se si inseriscono anche dei *tag* con nomi e cognomi.

**2. Geolocalizzati? No, grazie.** Per gli amanti della riservatezza che non vogliono mai 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* eventualmente utilizzati.

**3. Social-ladri.** Postando sui *social network* che si è in vacanza si potrebbe far sapere ad eventuali malintenzionati che la propria casa è vuota. Il pericolo aumenta se poi si scrive anche per quanto tempo si resterà in vacanza o in quali giorni. Il suggerimento è innanzitutto quello di evitare di postare sul web informazioni troppo personali, come l'indirizzo di casa o la foto del posto dove si parcheggia di solito l'automobile. E' bene poi controllare le impostazioni privacy dei *social network*, limitando la visibilità dei *post* solo agli amici; fare attenzione a non accettare sconosciuti nella cerchia di amicizie on-line; eventualmente, bloccare la funzione di geolocalizzazione dei *social network* per non far sapere quanto si è lontani dalla propria abitazione.



**4. Viaggi o "pacchi"?** E' bene fare attenzione alle offerte di sconti straordinari su viaggi e affitti di case per le vacanze - da ottenere compiendo determinate operazioni, come, ad esempio, cliccare su *link*, fornire dati personali o bancari - che possono arrivare via *social network*, *e-mail*, *sms*, sistemi di messaggistica. Virus informatici, software spia e *phishing* (cioè, una frode finalizzata all'acquisizione, per scopi illegali, di dati personali dell'utente) possono essere in agguato. Inoltre, per evitare i rischi di furti di identità, meglio essere prudenti con i pagamenti on-line se l'indirizzo internet del sito appare anomalo (ad esempio, se non corrisponde al nome dell'azienda che dovrebbe gestirlo) o se non 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).

**5. Attenzione alle app.** In vacanza molti utenti di *smartphone* e *tablet* scaricano *app* per giochi, suggerimenti turistici, ecc.. Ma questi prodotti software 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; evitare che i minori possano scaricare le *app* da soli.

**6. Wi-fi gratuito, ma con prudenza.** Le connessioni offerte da locali, 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 internet, meglio evitare di usare servizi che richiedono credenziali di accesso (ad esempio, alla propria *webmail*, ai *social network*, ecc.) o fare acquisti online utilizzando il *web banking* o la carta di credito.



**7. Navigare protetti.** 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, non solo quando si usa il pc, ma anche per *smartphone* e *tablet*. E' bene mantenere aggiornati anche i sistemi operativi di tutti i dispositivi utilizzati per garantirsi una maggiore protezione.



**8. Smartphone e tablet sicuri.** Durante le vacanze, purtroppo, può accadere che *smartphone* e *tablet* siano smarriti o vengano rubati. Per proteggere i dati che contengono, conviene impostare un codice di accesso non banale 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. In generale, è bene non conservare dati troppo personali su *smartphone* e *tablet* (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*). Prima di partire si potrebbe fare un *backup* di tutte le informazioni (numeri di telefoni, foto, ecc.) su "chiavette" o hard disk esterni, oppure trasferirli sul *cloud*. Ovviamente, in quest'ultimo caso, è bene informarsi sulle condizioni contrattuali e sulle garanzie privacy del servizio *cloud*.

**9. Sms e messaggi via smartphone e social network.** Nel periodo estivo se ne inviano e se ne ricevono molti. Alcuni potrebbero contenere virus, *malware* o esporre al rischio di *spam*. E' sempre bene fare molta attenzione prima di scaricare programmi, aprire eventuali allegati o cliccare *link* contenuti nel testo o nelle immagini dei messaggi. 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.

**10. La miglior difesa** è usare sempre con consapevolezza e attenzione le nuove tecnologie e gestire con accortezza i nostri dati personali.

Per maggiori informazioni, è possibile consultare anche la sezione [Diritti e Prevenzione](#) del sito web [www.garanteprivacy.it](http://www.garanteprivacy.it) e le campagne di comunicazione del Garante "[Fatti smart](#)", "[Connetti la testa](#)" e "[Spam: come difendersi](#)".

E' inoltre possibile rivolgersi per informazioni, chiarimenti o segnalazioni all'[Ufficio Relazioni con il Pubblico \(URP\)](#) del Garante.

Roma, 5 luglio 2014