

Privacy, su selfie e dintorni scende in campo il Garante: il decalogo per l'estate "sicura"

di **Redazione**

02 Agosto 2014 - 17:27



#Setiselfieticancello. E' la campagna "social" (e sociale) per i cosiddetti "selfie-addicted", ideata da Davide Ferazza e Alessio Fava con un [video](#), subito diventato virale e riproposto anche dalla rivista Wired, prodotto da Withstand film. Sottotitolo, "il prossimo a sparire dal mio Facebook potresti essere tu". E chi, del resto, non ha tra i propri contatti un amico/a le cui foto auto-scattate compaiono sempre più spesso sulla bacheca? La selfie-mania, le cui derive sono già oggetto di studi psicosociali, non è solo una questione di moda e di mordace ironia. E' il Garante della Privacy in persona a scendere in campo sulla questione, mettendo in guardia contro l'ormai celebre autoscatto, e più in generale contro gli errori da evitare in materia di privacy, soprattutto nel periodo estivo.

Si chiama, e non a caso, "La Privacy sotto l'ombrellone. Consigli per navigare sicuri durante le vacanze estive" il decalogo del Garante stilato per le ferie 2.0 degli italiani diffuso a inizio luglio. Al primo punto c'è proprio "Selfie e dintorni".

“Pubblicare le foto o i video delle vacanze sui social network è divertente - si legge - 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”.

Secondo e terzo, i consigli su geolocalizzazione (il suggerimento è disattivare le opzioni di geolocalizzazione di smartphone e tablet, oltre a quelle dei social network se non si vuol far sapere al mondo in che parte di esso si è). Perché, ricorda il Garante, ad approfittarne potrebbero esserci i “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”. Suggerimento: evitare di postare sul web informazioni troppo personali, (indirizzo di casa o la foto del posto dove si parcheggia di solito l'automobile), e controllare le impostazioni privacy dei social network, evitando di avere sconosciuti tra la cerchia di amici.

Seguono i consigli su come evitare furti di identità, pagamenti on line sospetti, truffe, software spia e phishing, virus e malware nascosti sia nei link sia nelle app per giochi, suggerimenti turistici, ecc..

Anche il wifi gratuito, sempre accolto con gioia dagli utenti, potrebbe nascondere insidie. “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. 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 on-line utilizzando il web banking o la carta di credito”.

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, ricorda l'autorità garante.

Inoltre 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 (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”.

Infine “la miglior difesa”: usare sempre con consapevolezza e attenzione le nuove tecnologie e gestire con accortezza i nostri dati personali.