Consigli per navigare sicuri durante le feste natalizie

1. Uso intelligente dei social network. Se durante le feste di Natale si parte per le vacanze, bisogna fare attenzione a non comunicare sul web per quanto tempo non si sarà in casa e in quali giorni. In ogni caso, è sempre bene evitare di postare informazioni riguardanti l'indirizzo di casa, il posto dove si parcheggia di solito o la targa dell'auto. I malintenzionati sono sempre in agguato…

2. Occhio agli Sms con auguri e offerte di Natale. Nell'epoca degli smartphone, i messaggi Sms possono contenere anche virus, link a servizi indesiderati a pagamento e programmi potenzialmente dannosi per la privacy. E' buona regola limitare la diffusione del proprio numero telefonico e non rispondere a messaggi provenienti da numeri sconosciuti.

3. Cartoline di auguri elettroniche. Fa piacere riceverle e spedirle via e-mail, Sms, Mms e social network. Ma possono contenere virus, malware (cioè programmi dannosi) 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. Si possono poi adottare semplici precauzioni: ad esempio, non rispondere alle e-mail provenienti da sconosciuti, oppure passare il mouse su un link senza cliccarlo e verificare - in basso a sinistra nel browser - la Url (cioè, l'indirizzo web) reale al quale si potrebbe essere indirizzati.

4. Truffe e posta elettronica. Diffidare delle offerte di sconti straordinari su viaggi e regali da ottenere compiendo determinate operazioni (ad esempio, cliccare su link, fornire dati personali o bancari, ecc.), che possono arrivare via social network, e-mail o Sms. Malware, virus informatici, software spia e phishing (cioè, una frode finalizzata all'acquisizione, per scopi illegali, di dati riservati dell'utente) possono essere in agguato. Anche qui, valgono le stesse precauzioni indicate per le cartoline elettroniche. Un pericolo in crescita nel periodo delle feste è quello delle false notifiche di spedizione, che avvisano dell'aggiornamento di un ordine mai effettuato o

della necessità di ritirare un pacco. Nei casi dubbi, quando non si è effettuato alcun ordine e non si attende alcuna consegna, è bene evitare di fornire dati personali online, e non cliccare link sospetti o installare eventuali software indicati come necessari per completare le operazioni di spedizione e consegna. Le aziende del settore, infatti, operano abitualmente tramite altri canali.

5. Attenzione alle app. Durante le feste molti utenti di smartphone e tablet scaricano app gratuite per avere accesso a promozioni o negozi online, per creare e inviare cartoline di Natale o attivare giochi. Questi prodotti software possono anche nascondere virus o malware. Per proteggersi, buone regole sono: scaricare le app dai market ufficiali; leggere con attenzione le descrizioni dei programmi; consultare eventuali recensioni degli utenti; evitare che i minori possano scaricare le app da soli.

6. Falsi siti. Diffidare dello shopping online troppo scontato se non si è sicuri dell'affidabilità del sito, se l'indirizzo Internet del sito appare anomalo (ad esempio, se non corrisponde al nome dell'azienda che dovrebbe gestirlo) e se non vengono rispettate le procedure di sicurezza standard per le transazioni online (protocolli https). In ogni caso, è sempre bene fare estrema attenzione quando vengono richieste le credenziali della carta di credito o del conto bancario.

7. In vacanza, Wi-Fi gratuito ma con prudenza. Le connessioni offerte da locali e hotel potrebbero non essere protette e rendere pc, smartphone e tablet esposti a intrusioni esterne da parte di malintenzionati a caccia di dati personali. Inoltre, connessioni "infettate" da virus e malware potrebbero invitare gli utenti a installare un software prima dell'utilizzo, esponendo i dispositivi collegati a rischio di phishing.

8. Le foto delle vacanze e i tag. Non tutti vogliono apparire sui social network, essere riconosciuti o far sapere dove e con chi si trovavano durante le feste natalizie. Se si postano delle foto con altre persone, è meglio prima accertarsi che siano d'accordo, specie se si inseriscono anche dei tag con nomi e cognomi.

9. Geolocalizzazione solo quando si vuole. Se invece si preferisce non far sapere dove si è durante le vacanze o le feste di Natale si possono disattivare le opzioni di geolocalizzazione di smartphone e tablet e quelle dei social network utilizzati.

10. Smartphone e tablet protetti. Aggiornamenti software costanti e programmi antivirus dotati anche di anti-spyware e anti-spam possono essere delle buone precauzioni per evitare furti di dati o violazioni della privacy. Ma è bene ricordare che le migliori difese sono la consapevolezza nell'uso delle tecnologie e l'accortezza nel diffondere i nostri dati personali.

Fonte: www.garanteprivacy.it