Natale in privacy

Suggerimenti su come tutelare i dati personali durante le Feste di Natale

1. Auguri a prova di privacy

Nel periodo natalizio si ricevono e si inviano molti **messaggi o cartoline d'auguri virtuali tramite sms**, sistemi di messaggistica, e-mail e social network.

Alcuni messaggi potrebbero però contenere virus, link a servizi a pagamento o tentativi di phishing e programmi potenzialmente dannosi, come ransomware o software spia.

E' quindi bene **fare attenzione prima di scaricare programmi, aprire eventuali allegati o cliccare su link** contenuti nel testo o nelle immagini presenti all'interno dei messaggi ricevuti. Specie se il messaggio arriva da soggetti sconosciuti o se il testo è strano e contiene grossolani errori di ortografia, grammatica, ecc..

(**VEDI ANCHE:** https://www.garanteprivacy.it/temi/cybersecurity)

2. Foto e video sotto l'albero

Non tutti vogliono apparire nelle foto di pranzi, cene e festeggiamenti che spesso si pubblicano online, essere riconosciuti o far sapere dove e con chi trascorrono le feste natalizie. **Se si postano foto o video in cui compaiono altre persone**, è sempre quindi meglio prima accertarsi che queste siano d'accordo, soprattutto se si inseriscono anche dei tag con nomi e cognomi.

Particolare attenzione va riservata alle foto e ai video in cui compaiono bambini. Occorre infatti ricordare che le immagini dei minori pubblicate online potrebbero essere visualizzate e scaricate anche da malintenzionati. Meglio quindi evitare quindi di "postarle", oppure almeno **limitare le impostazioni di visibilità delle immagini sui social network solo ai propri "amici**".

In alternativa, si possono utilizzare alcune accortezze, come **rendere irriconoscibile il viso del minore**, ad esempio, utilizzando programmi di grafica per inserire "pixel" sui volti (disponibili anche gratuitamente online) oppure semplicemente coprendolo con una "faccina" emoticon.

(**VEDI ANCHE:** https://www.garanteprivacy.it/temi/foto)

3. "Pacchi" di Natale

Diffidare delle offerte con sconti straordinari (su viaggi, abbigliamento, buoni e gift card, oggetti di vario genere) che è possibile ottenere solo a condizione di effettuare determinate azioni (ad esempio, cliccare su link, fornire dati personali o bancari, ecc.). Questi messaggi - che possono arrivare ad esempio via social network, e-mail, messaggistica, sms - sono purtroppo a volte inviati da malintenzionati che cercano di "infettare" i dispositivi con virus e programmi malevoli oppure provano ad accedere ai dati personali contenuti in smartphone e computer (a volte anche relativi al conto bancario o alla carta di credito).

Per proteggersi, è sempre meglio fermarsi un momento a riflettere e non accettare di istinto le azioni richieste; e magari, nei limiti del possibile, fare dei controlli, verificando ad esempio se il messaggio corrisponde ad un sito affidabile, se ci sono notizie online sull'affidabilità del venditore, ecc..

(VEDI ANCHE: https://www.gpdp.it/temi/cybersecurity)

Un pericolo che aumenta nel periodo delle feste è quello delle **false notifiche di spedizione**, che avvisano dell'aggiornamento di un ordine o della necessità di ritirare un pacco. Nei casi dubbi, quando non si è effettuato alcun acquisto e non si attende alcuna consegna, è bene **evitare di fornire dati personali online e non aprire 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.

In generale, se si utilizzano **servizi online per fare regali o per prenotare vacanze**, è più prudente usare **carte di credito prepagate** o altri **sistemi di pagamento che permettono di evitare la condivisione di dati del conto corrente o della carta di credito**. E' inoltre utile impostare avvisi (alert) per essere a conoscenza in tempo reale delle transazioni che avvengono sul conto o sulla carta di credito e accorgersi di eventuali addebiti non autorizzati per poter intervenire rivolgendosi subito alla propria banca o al gestore della carta.

Altra importante accortezza è **controllare l'indirizzo internet dei siti su cui si fanno pagamenti online**: in particolare, verificare se corrisponde al nome dell'azienda che dovrebbe gestirlo e se vengono rispettate le procedure di

sicurezza standard per i pagamenti online (ad esempio, la URL - cioè l'indirizzo - del sito deve iniziare con "https" e avere il simbolo di un lucchetto).

4. App senza sorprese

Durante le feste molti utenti scaricano app gratuite per avere accesso a promozioni o negozi online, per creare e inviare cartoline di Natale, per avere uno screensaver natalizio dello smartphone o del computer, per attivare giochi.

Alcune applicazioni potrebbero però anche nascondere virus o malware.

Per proteggersi, buone regole sono:

- prima di installare una APP, cercare di capire quanti e quali dati verranno raccolti e come verranno utilizzati, **consultando l'informativa sul trattamento dei dati personali;**
- scaricare le app solo 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** di altri utenti nell'uso di una determinata app, di una piattaforma per il download di film, di un sito, ecc. per verificare se sono segnalati problemi riguardanti la sicurezza dei dati;
- 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.

(**VEDI ANCHE:** https://www.garanteprivacy.it/app)

5. Se parti non lasciare il buonsenso a casa

Se durante le feste di Natale si parte per le vacanze, meglio **evitare di pubblicare sui social media informazioni che possono rivelare per quanto tempo si sarà assenti e in quali giorni**: potrebbero essere utili a eventuali malintenzionati. In ogni caso, è sempre bene evitare di diffondere online informazioni che permettono di individuare l'indirizzo di casa o il posto dove di solito si parcheggia l'auto.

Se sono presenti in casa **prodotti e sistemi domotici**, è importante ricordare che questi dispositivi possono essere esposti ad attacchi informatici, virus e malware. E' quindi bene assicurarsi che siano protetti, ad esempio impostando password robuste e aggiornando costantemente il software per garantire una maggiore protezione.

Prima di partire meglio spegnere o disconnettere i dispositivi smart non indispensabili. Per quelli che restano operativi, si possono eventualmente impostare sistemi di alert per controllare a distanza il loro funzionamento e monitorare anche lo stato della propria abitazione.

6. In albergo o al ristorante, Wi-Fi gratuito ma con prudenza

Durante una vacanza natalizia è bene ricordare che le **connessioni offerte da locali e hotel** potrebbero non essere protette e rendere pc, smartphone e tablet esposti a virus, software malevoli o intrusioni esterne da parte di malintenzionati a caccia di dati personali.

Se non si è certi degli standard di sicurezza del wi-fi gratuito offerto dai luoghi che ci ospitano, è opportuno adottare sempre alcune accortezze, come evitare di accedere a servizi online che richiedono credenziali di accesso (ad esempio, la propria webmail, i social network, il conto corrente, ecc.) o fare acquisti online con la carta di credito.

7. Se il drone viene in vacanza con noi

Se si fa volare a fini ricreativi un drone munito di fotocamera nei luoghi delle vacanze natalizie, ad esempio in montagna o al mare, è bene evitare di invadere gli spazi personali e la riservatezza delle persone.

Sul tema il Garante mette a disposizione una scheda informativa con suggerimenti per un divertimento a prova di privacy: https://www.garanteprivacy.it/temi/droni.

8. Giocattoli smart, privacy smart

Se per Natale si decide di regalare ai più piccoli uno **smart toy**, cioè un giocattolo intelligente e interattivo, occorre ricordare che questi dispositivi divertenti e spesso anche educativi possono raccogliere e trattare dati personali degli utilizzatori piccoli e grandi.

Sul tema è utile consigliare anche le pagine informative www.gpdp.it/minori e www.gpdp.it/iot/smarttoys.

9. Proteggi i tuoi dispositivi

Aggiornamenti software costanti e programmi antivirus dotati anche di anti-spyware e anti-spam possono costituire buone precauzioni per evitare furti di dati o violazioni della privacy di smartphone, tablet e pc.

E’ utile consultare la pagina informativa del Garante sul tema: https://www.garanteprivacy.it/cybersecurity

10. La miglior difesa

E' sempre importante ricordare che le migliori difese da possibili violazioni della nostra privacy sono la consapevolezza nell’uso delle tecnologie e l’accortezza nel diffondere i nostri dati personali.

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

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