

03.07.2026

A cosa bisogna fare attenzione sui dispositivi mobili durante le vacanze estive?

Le vacanze sono sinonimo di relax, prenotazioni all'ultimo minuto, navigazione, condivisione di foto od operazioni rapide sul portale dell'e-banking – molte di queste cose oggi si fanno direttamente dallo smartphone o dal tablet. Proprio per questo motivo durante le vacanze i criminali informatici si concentrano in particolare sui dispositivi mobili.

La noncuranza mentre si è in viaggio può facilmente tradursi in perdite di dati, account crackati o danni finanziari. Bastano pochi accorgimenti, però, per ridurre sensibilmente i rischi.

Prima del viaggio: preparare i dispositivi

Prima della partenza è opportuno controllare e preparare i dispositivi mobili:

- Installate gli ultimi aggiornamenti della sicurezza per il sistema operativo e le app.
- Eliminate le app non necessarie o gli account utente vecchi.
- Create un backup aggiornato dei vostri dati e delle vostre foto.
- Attivate il blocco del dispositivo con il PIN, l'impronta digitale o il riconoscimento facciale.
- Attivate funzioni come «Trova il mio iPhone» o «Trova il mio dispositivo».
- Salvate i numeri di telefono importanti in un archivio separato.
- A seconda della destinazione, è consigliabile portarsi soltanto un secondo cellulare, con le funzioni più essenziali, e lasciare al sicuro a casa il dispositivo principale privato.

Soprattutto quando si è in viaggio, uno smartphone smarrito o rubato può trasformarsi in un grosso problema. Ancor di più se ci sono memorizzati dati di pagamento, e-mail o dati di accesso.

Attenzione alle reti WLAN pubbliche

La connessione WLAN gratuita in albergo, negli aeroporti o nei bar è pratica, ma spesso non è sicura. I criminali informatici possono infatti tentare di intercettare i dati o predisporre hotspot falsi.

Attenzione quindi:

- Utilizzate il più possibile la rete dati mobile.
- Collegatevi solo alla rete WLAN ufficiale dell'hotel o del ristorante.
- Evitate di effettuare attività sensibili come l'e-banking attraverso le reti pubbliche.
- Disattivate le connessioni WLAN automatiche.

Una VPN (Virtual Private Network) può offrire una protezione aggiuntiva, ma non sostituisce la prudenza nel proprio

comportamento.

Le vacanze sono l'alta stagione per il phishing

Durante le vacanze estive si moltiplicano le notizie fraudolente riguardanti viaggi, prenotazioni o consegne di pacchi; casi sempre frequenti sono in particolare:

- contraffazione di una conferma di prenotazione
- presunti problemi con le carte di credito
- SMS o messaggi WhatsApp che informano di presunte modifiche ai voli
- falsi messaggi da hotel e agenzie di viaggio

Non fate clic sui link con disattenzione e non aprite allegati sospetti. Esaminate sempre con occhio critico mittenti e siti Internet.

Attenzione alle stazioni di ricarica USB

Le stazioni di ricarica USB pubbliche, presenti negli aeroporti o nelle stazioni ferroviarie, possono essere manomesse. C'è allora il rischio che i dati vengano letti o che venga installato del software dannoso («juice jacking»).

È dunque più sicuro usare:

- un proprio caricabatterie
- una normale presa di corrente
- una power bank

Dopo il viaggio: fare un controllo

Dopo le vacanze si consiglia di effettuare un breve controllo di sicurezza:

- Controllate le operazioni del conto e delle carte di credito.
- Eliminate le app di viaggio e gli account utente che non vi servono più.
- Cambiate le password di account importanti se avete utilizzato reti pubbliche.
- Controllate i dispositivi abilitati e gli accessi dei vostri principali servizi online.

Ulteriori suggerimenti su come utilizzare il dispositivo mobile in modo sicuro quando siete in viaggio sono disponibili qui: www.ebas.ch/holidaycheck (<https://www.ebas.ch/it/vacanze-viaggi/>)