



Turismo - Turismo, Federconsumatori: stagione dei viaggi parte all'insegna della truffa, attenzione a false richieste di pagamento e link sospetti

Roma - 24 apr 2025 (Prima Notizia 24) I consigli di Federconsumatori su come difendersi dalle truffe.

“Molti italiani sono in partenza per il ponte del 25 aprile e del 1 maggio, il 16,2% degli italiani secondo le stime dell'O.N.F. – Osservatorio Nazionale Federconsumatori. Con l'avvio della “stagione calda” delle partenze, però, aumentano anche le truffe che hanno nel mirino proprio i cittadini che si apprestano a mettersi in viaggio. In questi giorni stiamo ricevendo presso i nostri sportelli numerose segnalazioni di e-mail truffa, che imitano noti portali, soprattutto Booking.com, chiedendo di effettuare nuovamente pagamenti non andati a buon fine. Le e-mail giungono pochi giorni prima della partenza, soprattutto a chi ha prenotato soggiorni all'estero. Invitiamo i cittadini a prestare la massima attenzione: si tratta di truffe, che riproducendo grossolanamente la grafica di noti portali, reindirizzano i pagamenti su altri siti, spesso privi di ogni basilare parametro di sicurezza. Nel caso aveste ricevuto e-mail simili non cliccate sul link proposto ma contattate la struttura ricettiva, direttamente o tramite la piattaforma su cui avete prenotato. Nel caso in cui abbiate cliccato, o ancora peggio effettuato un doppio pagamento, contattate la sede della Federconsumatori più vicina per ricevere assistenza, oppure il nostro sportello dedicato SOS Turista al numero 059 251108 o all'indirizzo e-mail info@sosvacanze.it”. Lo rende noto Federconsumatori. La Federazione ricorda alcuni consigli utili per difendersi in caso di phishing e smishing, tipologie di truffa molto diffuse in ambito turistico e non solo. Phishing: i truffatori inviano e-mail che sembrano provenire da fonti affidabili, come banche, agenzie di viaggio, noti portali di prenotazione, imitandone in tutto e per tutto la grafica, chiedendo informazioni personali e finanziarie degli utenti, doppi pagamenti, cauzioni o garanzie. Smishing: in questo caso i raggiri viaggiano via SMS. I messaggi sono creati ad arte per ingannare i viaggiatori, spingendoli a cliccare su link pericolosi, che sottraggono informazioni personali, rimandano anche in questo caso a richieste di pagamento o fanno partire il download di virus e malware. Come difendersi? - Non cliccare mai su link sospetti e non fornire informazioni personali o finanziarie in risposta a e-mail o SMS non richiesti; - Utilizzare solo i canali ufficiali per comunicare con la propria banca o con i fornitori di servizi di viaggio; - Controllare nel dettaglio l'indirizzo e-mail del mittente; - Nel caso si tratti di SMS o MMS, controllare che il mittente non sia un numero di cellulare qualsiasi, ma un Alias registrato sul portale Agcom (<https://alias.agcom.it/index.php>). - Una volta accertata l'autenticità del messaggio, prima di cliccare su qualsiasi link, verificare sempre la sicurezza dell'indirizzo web assicurandosi che sia preceduto da “https://”.



(Prima Notizia 24) Giovedì 24 Aprile 2025

PRIMA NOTIZIA 24

Sede legale : Via Costantino Morin, 45 00195 Roma
E-mail: redazione@primanotizia24.it