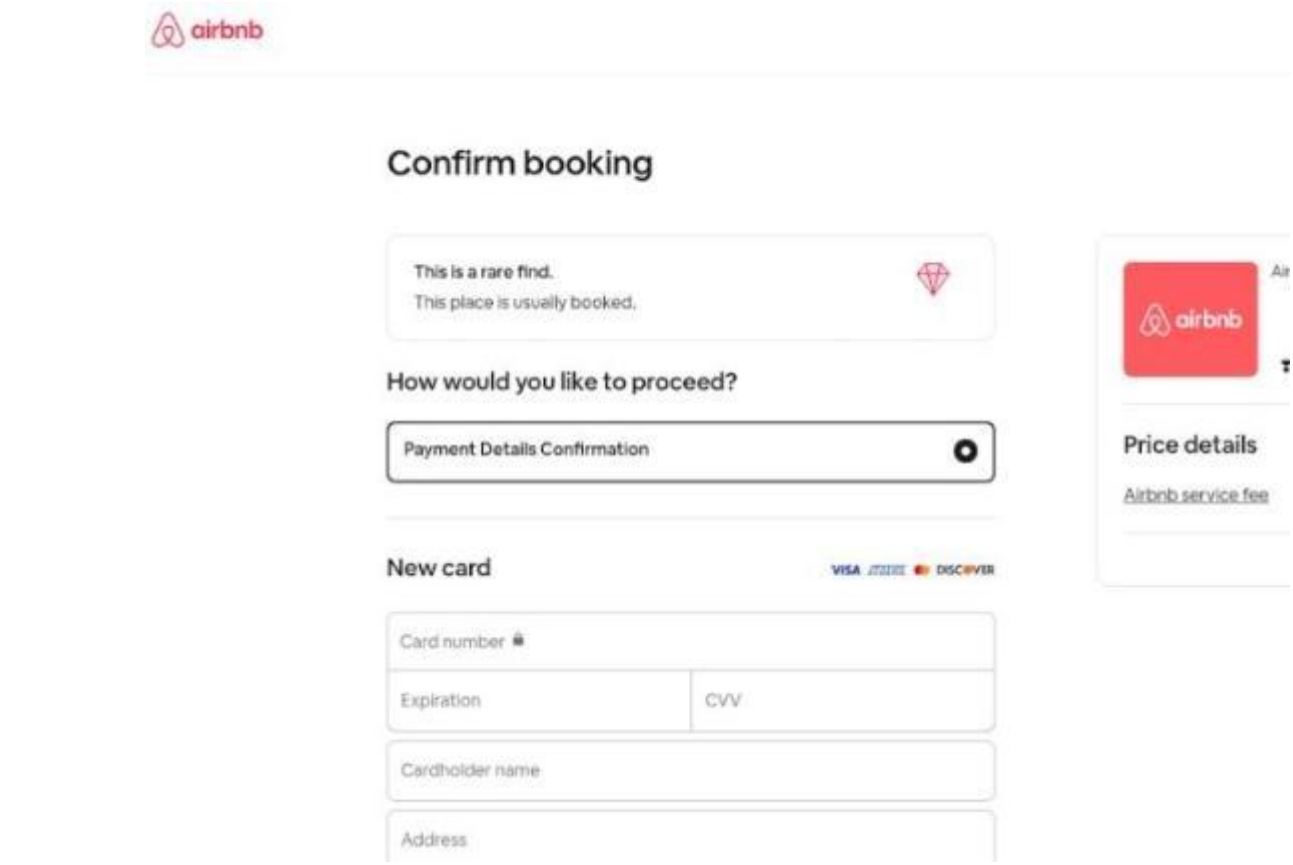
Finti Booking e Airbnb, è boom di siti truffa legati alle vacanze: come difendersi dal phishing estivo

Quest'anno simili raggiri stanno facendo registrare un'«impennata». Lo si legge in un report di Check Point Software che include anche cinque consigli utili per riconoscere trappole del periodo prima che sia troppo tardi (Fonte: https://www.corriere.it/ 24 giugno 2025)

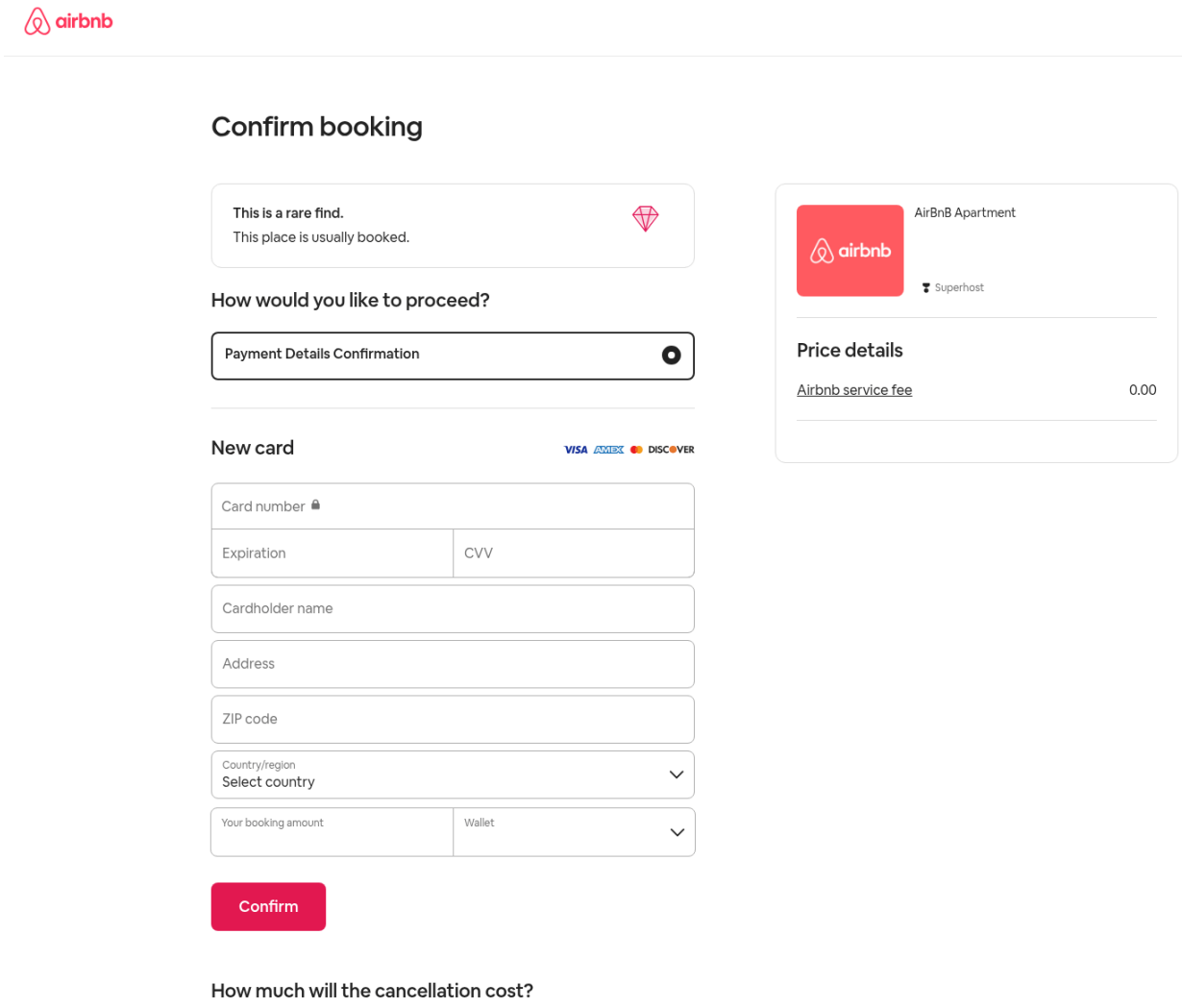


Non passa estate senza che qualcuno, in Italia e non solo, incappi in qualche **truffa informatica legata alle vacanze**. Caso tipico, quello di chi giunge nella tanto agognata meta delle ferie per poi scoprire che la casa che aveva prenotato non esiste. Alla base del raggiro, annunci fasulli spesso veicolati con il meccanismo del phishing, che consiste nell'**inviare alle vittime un messaggio contraffatto** e, attraverso l'indebito utilizzo del nome e del logo del presunto mittente – banche, aziende, istituzioni –, convincerle a rivelare dati riservati o a compiere una determinata azione. Ebbene, non solo il copione ha già iniziato a ripetersi puntuale anche quest'anno, ma gli esperti di Check Point Software Technologies, fornitore internazionale di piattaforme di cybersecurity basate sull'intelligenza artificiale per aziende e governi, stanno perfino rilevando un'autentica «**impennata di siti web ingannevoli**». Mentre infatti a maggio 2024 avevano classificato come «**malevolo o sospetto**» un dominio su 33 tra quelli appena creati a livello globale in tema ferie o vacanze, **il mese scorso tale incidenza è salita a uno su 21**.

Il falso form di pagamento

Primo esempio di truffa nei confronti del quale la nuova indagine raccomanda di tenere gli occhi aperti, quello dei **falsi form di pagamento**. Guardare l'immagine al termine di questo paragrafo

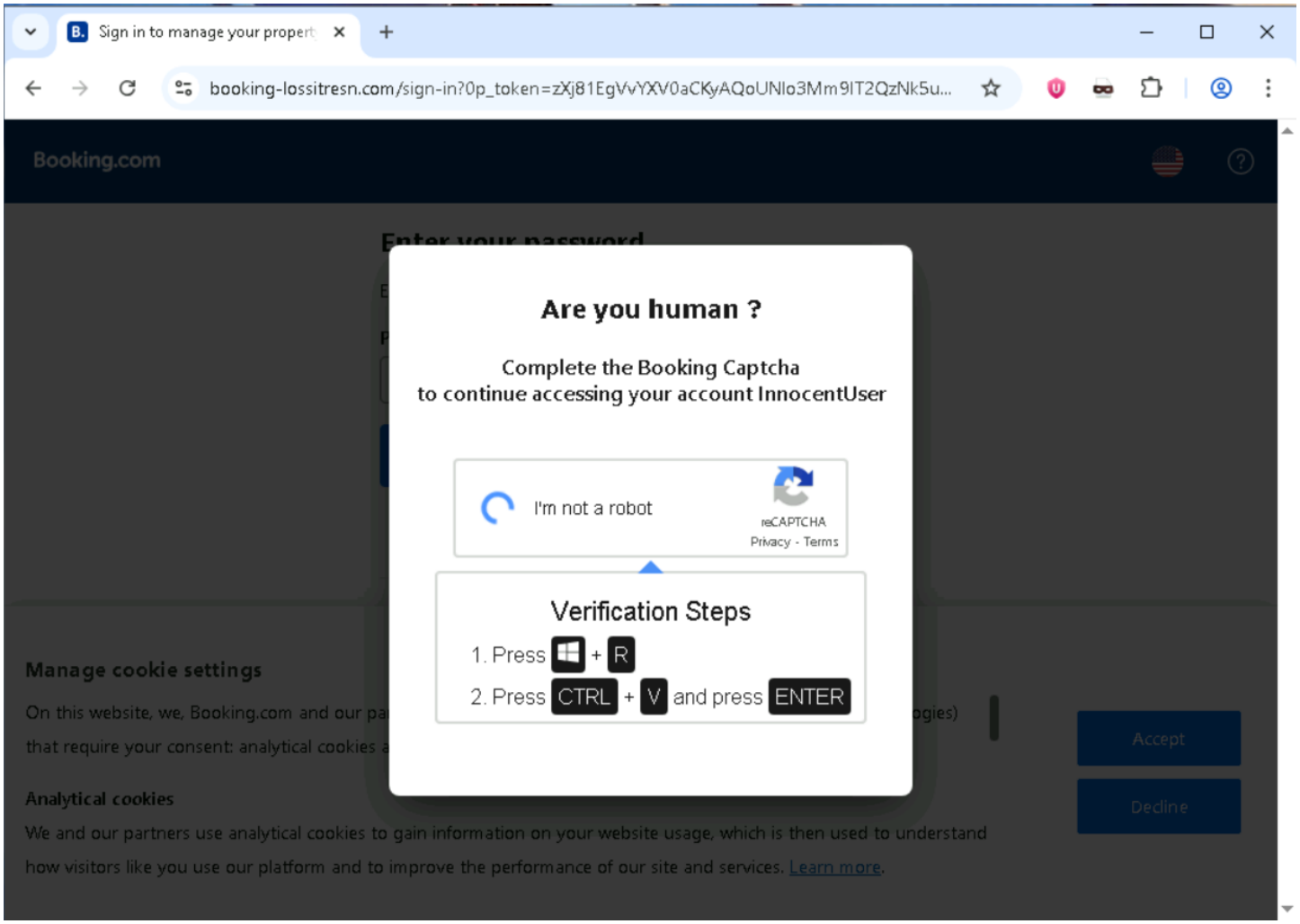
per credere: sembrerebbe una «normale» pagina web di Airbnb, popolarissima piattaforma dedicata agli affitti brevi. È invece un **sito fraudolento dall'Url ben diverso** che, creando una falsa sensazione di legittimità – recita il report –, attira le vittime inducendole a inserire i propri dati di pagamento per **rubare le informazioni sensibili come i numeri di carta, il CVV e la data di scadenza**». Ovvie perciò le conseguenze che cadere nel tranello potrebbe comportare sul conto in banca.



Fonte: Check Point Software Technologies

Il falso accesso per gli host

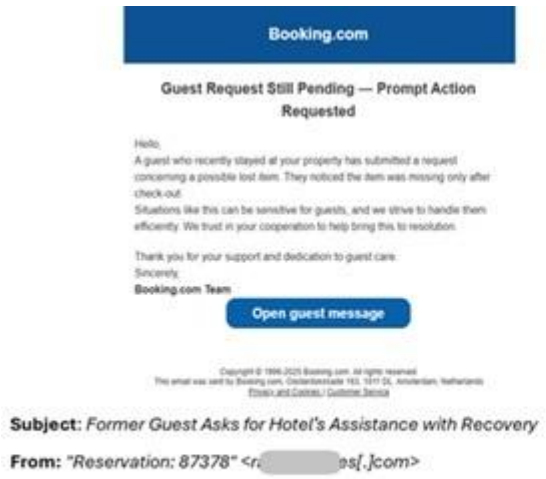
Altro brand del settore illegalmente imitato dai cybercriminali, l'altrettanto conosciuto **Booking.com**. Il quale, se da un lato può essere impiegato per truffare i vacanzieri usando lo stesso schema appena descritto, dall'altro – evidenzia l'indagine – viene sfruttato **anche a potenziale danno degli host**. Due, in questo caso, le procedure messe sotto la lente d'ingrandimento. Nella prima «il sito fraudolento imita la pagina di login di booking.com dal lato del proprietario della struttura», poi fa apparire «un **falso ReCAPTCHA** per "verificare" se si tratta di un essere umano», infine chiede «di eseguire ulteriori azioni premendo il tasto Windows + R, Ctrl + V e Invio». Obiettivo: **far innescare all'utente «uno script PowerShell** che scarica un payload RAT (AsyncRAT) da un server C2 e lo installa sul computer», violandone così le difese.



Fonte: Check Point Software Technologies

La falsa email di un ospite

Seconda procedura fraudolenta indirizzata agli host di Booking.com, una **massiccia campagna di email** atte a informare che «un ospite aveva inviato un messaggio all'albergatore riguardo a un oggetto forse smarrito». Sotto questo profilo – si apprende –, «ogni email richiedeva la stessa azione: **rivedere la richiesta dell'ospite**». In che modo? Cliccando su un apposito link, naturalmente: quello di un altro sito «clone» dell'originale, messo a punto dai malintenzionati digitali per fare incetta di dati sensibili. Non bastasse – scrivono gli esperti –, «un'analisi più attenta delle email di phishing mostra un'**ampia varietà di soggetti e contenuti**, pur mantenendo ben chiaro lo stesso tema. Anche il testo del pulsante varia da un'email all'altra. Questo potrebbe indicare l'utilizzo di **strumenti di intelligenza artificiale generativa**»: un'arma in più, rispetto a qualche tempo fa, per tranne in inganno gli utenti.



Fonte: Check Point Software Technologies

I consigli per difendersi

«Che si sia viaggiatori che pianificano la prossima avventura o aziende che proteggono i dati dei clienti, **le misure di sicurezza proattive sono essenziali** – spiegano gli autori del report –. Dal momento che le truffe di phishing diventano sempre più sofisticate e opportunistiche, **comprendere il panorama delle minacce e sapere come reagire può fare la differenza tra una vacanza sicura e una compromessa**». Cinque, in questo senso, i loro principali suggerimenti per assicurarsi «una buona igiene informatica durante la stagione delle vacanze». **Eccoli in chiusura**, a garanzia della possibilità di godersi appieno lo spensierato relax che dovrebbe contraddistinguere il periodo.

- **Prenotare direttamente da fonti ufficiali**. Digitare sempre manualmente l'indirizzo del sito web o utilizzare applicazioni affidabili, evitando di cliccare sui link contenuti nelle e-mail o nei messaggi.
- **Ricontrollare gli Url**, verificando eventuali errori di ortografia o terminazioni di dominio insolite (ad esempio,.today, .info), spesso utilizzate nei siti di truffa.
- **Attivare l'autenticazione a più fattori (Mfa)**. Questo aggiunge un ulteriore livello di sicurezza anche se le credenziali di accesso sono compromesse.
- **Essere prudenti con il Wi-Fi pubblico**, utilizzando una VPN quando accedete a informazioni sensibili come conti bancari o portali di prenotazione.
- **Installare la sicurezza degli endpoint**. Una protezione completa per dispositivi mobili e desktop può rilevare i tentativi di phishing e bloccare i download dannosi in tempo reale.

Truffe telefoniche e online, notizie e approfondimenti

Truffe in vacanza, dalle prenotazioni ai bonifici: le 8 regole per ridurre i rischi. La guida di Polizia e Airbnb