**ITA**

**Gentile Ospite,**

il tempo della tua vacanza si sta avvicinando e la nostra missione è di farti trascorrere un soggiorno spensierato.

Per questo abbiamo a cuore la tua sicurezza - anche digitale: se hai prenotato tramite piattaforme online, come Booking.com, ti ricordiamo di **non cliccare su link esterni** ricevuti nella chat di **Booking.com** e di **non inserire mai i dati della tua carta di credito nella chat**. Queste accortezze aiutano a proteggerti da possibili tentativi di truffa.

**Cosa fare se ricevi un messaggio sospetto:**
✔️ Non lasciarti prendere dal panico per la tua vacanza e **non rispondere** a richieste sospette prima di aver verificato che il messaggio sia autentico.
✔️ Booking.com consiglia: *“Controlla sempre due volte le politiche di pagamento della struttura elencate nella pagina di prenotazione o nell'e-mail di conferma. Se non è indicata alcuna richiesta di pagamento anticipato o deposito, ma ti viene chiesto di pagare in anticipo per garantire la prenotazione, è probabile che si tratti di una truffa.”*
✔️ In caso di dubbi, **contatta il servizio clienti di Booking.com e/o la nostra struttura direttamente**.
✔️ **Diffida di qualsiasi link** ti venga inviato: i pagamenti autentici avvengono esclusivamente tramite l'app o il sito ufficiale di Booking.com.
✔️ Fai attenzione a **messaggi con toni urgenti**, errori di ortografia o grammatica: sono spesso segnali di frode.
✔️ Se hai già inserito i dati della tua carta su un sito sospetto, **contatta subito il tuo fornitore di carta** per bloccarla o sostituirla.
✔️ Booking.com raccomanda anche di attivare **l’autenticazione a due fattori** per una maggiore sicurezza del tuo account.

Per maggiori informazioni, puoi consultare questo articolo di approfondimento:
👉 [The Guardian – Booking.com Scam](https://www.theguardian.com/money/2025/jun/29/your-reservation-is-at-risk-beware-the-bookingcom-scam)

Grazie per la collaborazione e buona vacanza!
**[Nome della struttura]**

**DEU**

**Lieber Gast,**
dein Urlaub rückt näher und unser Ziel ist es, dir einen unbeschwerten Aufenthalt zu ermöglichen.

Deshalb liegt uns deine Sicherheit — auch online — sehr am Herzen. Wenn du über Plattformen wie Booking.com gebucht hast, bitte **vermeide**, **auf externe Links im Booking.com-Chat zu klicken und deine Kreditkartendaten im Chat einzugeben**.
Diese einfachen Vorsichtsmaßnahmen helfen dir, dich vor möglichen Betrugsversuchen zu schützen.

**Bei einer verdächtigen Nachricht solltest du:**
✔️ Keine Panik wegen deines Urlaubs bekommen – überprüfe **vor deiner Beantwortung**, ob die Nachricht echt ist.
✔️ Booking.com empfiehlt: „*Überprüfe immer die Zahlungsrichtlinien der Unterkunft auf der Buchungsseite oder in der Bestätigungs-E-Mail. Wenn dort keine Vorauszahlung oder Kaution verlangt wird, du aber dennoch aufgefordert wirst, im Voraus zu zahlen, handelt es sich wahrscheinlich um Betrug*.“
✔️ Bei Unsicherheit: **Wende dich an den Kundenservice von Booking.com bzw. direkt an unsere Unterkunft.**
✔️ **Sei vorsichtig bei Links**, die dir zugesendet werden: echte Zahlungen erfolgen ausschließlich über die offizielle Booking.com-Website oder App.
✔️ Achte auf **Nachrichten mit Dringlichkeit**, Rechtschreib- oder Grammatikfehlern – das sind oft Anzeichen für Betrug.
✔️ Wenn du deine Kreditkartendaten bereits auf einer verdächtigen Seite eingegeben hast, **kontaktiere sofort deinen Kartenanbieter**, um die Karte zu sperren oder auszutauschen.
✔️ Booking.com empfiehlt außerdem**, die Zwei-Faktor-Authentifizierung** zu aktivieren, um dein Konto zusätzlich abzusichern.

Weitere Informationen findest du in diesem Artikel:
👉 [*The Guardian – Booking.com Scam*](https://www.theguardian.com/money/2025/jun/29/your-reservation-is-at-risk-beware-the-bookingcom-scam)

Vielen Dank für deine Aufmerksamkeit und einen schönen Urlaub!
**[Nome della struttura]**

**ENG**

**Dear Guest,**
your holiday is getting closer, and our mission is to make sure you enjoy a carefree stay.

That’s why your safety — including digital safety — is important to us. If you’ve booked through online platforms like Booking.com, please remember **not to click on external links sent in the Booking.com chat and never enter your credit card details in the chat**. These small precautions help protect you from potential fraud attempts.

**What to do if you receive a suspicious message:**
✔️ Don’t panic about your holiday and **avoid replying** to suspicious requests before verifying that the message is genuine.
✔️ Booking.com recommends: “Always double-check the payment policies of the property listed on the booking page or in the confirmation email. If no advance payment or deposit is mentioned, but you are asked to pay in advance to secure the booking, it is likely a scam.”
✔️ If in doubt, **please contact Booking.com Customer Service and/or reach out to our property directly**.
✔️ **Be cautious of any links sent to you**: legitimate payments are made only through the official Booking.com website or app.
✔️ Watch out for **messages with urgent tones**, spelling or grammar mistakes – these are often signs of fraud.
✔️ If you have already entered your card details on a suspicious site, please **contact your card provider immediately** to block or replace the card.
✔️ Booking.com also recommends enabling **two-factor authentication** for extra account security.

For more information, you can read this article:
👉 [*The Guardian – Booking.com Scam*](https://www.theguardian.com/money/2025/jun/29/your-reservation-is-at-risk-beware-the-bookingcom-scam)

Thank you for your cooperation and have a lovely holiday!
**[Nome della struttura]**