

【注意喚起】なりすましメールにご注意ください

平素よりフォーポイント フレックス by シェラトンをご利用いただき、誠にありがとうございます。

現在、オンライン宿泊予約サイト（以下、予約サイト）経由でご予約いただいたお客様に対し、ホテルや予約サイトの名前を騙ったフィッシング詐欺メールが確認されております。

このメールは、当ホテルや予約サイトのドメインとは異なる送信元アドレスから送られ、「予約確認」ボタンやリンクをクリックさせることで、クレジットカード情報などの個人情報盗取を目的としています。

当ホテルおよび Marriott International が、予約確認のためにお客様のクレジットカード情報の再入力や、外部リンク経由での「予約確認」を求めることは一切ございません。

以下のような特徴のメールにご注意ください。

- ・ 差出人アドレスが当ホテルの公式ドメインと異なる
- ・ 「WhatsApp で連絡したが返信がない」等の理由で緊急の確認を求める
- ・ 不審なリンク先への誘導、またはクレジットカード情報の入力を求める内容

不審なメールを受け取られた場合は、記載のリンクを開かず、添付ファイルを開かず、ご予約いただいた予約サイトのカスタマーセンターまで直接お問い合わせください。

セキュリティ対策として、各オンライン宿泊予約サイトにおけるパスワードの定期的な変更など、必要な対策を講じてまいります。

お客様には多大なご迷惑とご心配をおかけしておりますことを、深くお詫び申し上げます。

何卒ご理解いただき、ご注意賜りますようお願い申し上げます。

[Important Notice] Beware of Phishing Emails Impersonating Our Hotel

Thank you for choosing Four Points Flex by Sheraton.

We have become aware of phishing emails targeting guests who booked their stay through an online travel booking site (hereinafter "the booking site"). These emails impersonate our hotel or the booking site in an attempt to deceive guests.

These emails are sent from sender addresses that differ from the official domains of our hotel or the booking site. They attempt to trick recipients into clicking a "Confirm Booking" button or link, with the goal of stealing personal information such as credit card details.

Please note that neither our hotel nor Marriott International will ever ask guests to re-enter credit card information or "confirm" a booking via an external link.

Please be cautious of emails with the following characteristics:

- The sender's address differs from the official domain of our hotel or the booking site
- The email creates urgency by claiming, for example, that "we tried to contact you via WhatsApp but received no response"
- The email directs you to a suspicious link or asks you to enter credit card information

If you receive a suspicious email, please do not click any links or open any attachments. Instead, contact the customer service of the booking site directly.

As a security measure, we will be taking necessary precautions, including recommending regular password updates across online travel booking platforms.

We sincerely apologize for any inconvenience and concern this may have caused our guests.

We appreciate your understanding and ask that you remain vigilant against such fraudulent emails.