2023年12月27日

【重要なお知らせ】
（続報）Booking.com 管理システムへの不正アクセスによる個人情報流出の可能性とフィッシングサイトに誘導するメッセージ配信についてのお詫びとお知らせ

この度はBooking.com 管理システムへの不正アクセスによる個人情報流出について、お客様には多大なご迷惑およびご心配をおかけしておりますこと、深くお詫び申し上げます。

2023年10月6日に公表いたしました「【重要なお知らせ】Booking.com からの不正メールについて」につきまして、その後の調査により判明しました事実につきまして、以下のとおりご報告いたします。

10月6日付けお知らせ
【モンタン博多】お知らせ (montan.jp)

１．事象の経緯
2023年10月5日、「モンタン博多」の宿泊をBooking.com社を通じて予約された一部のお客様に対して、弊社の管理下にあるBooking.comサイト内に不正なアクセスがあり、フィッシングサイト等へ誘導するメッセージが配信されていたことが確認されました。また、管理システムに保存されているお客様の個人情報が第三者により閲覧された可能性があります。
その後、弊社から上記のメッセージが配信されたお客様へ注意喚起のメッセージを配信し、また、モンタン博多においてID・ログインパスワードの変更およびパソコンのセキュリティチェックを行っております。

2．事象の内容
（1）漏えいした可能性がある個人情報の件数
Booking.com社の管理システムに保存されている「モンタン博多」を予約したお客様の個人情報　680件

（2）漏えいした可能性があるお客さまの個人情報
氏名／電話番号／メールアドレス／国籍
※クレジットカード情報および金融機関口座情報などの決済関連情報は含まれておりません。

(3) 原因

専門会社にて原因調査を行った結果、管理システムへの不正アクセスを受けた原因は、システムの管理を行う「モンタン博多」の端末2台が2023年10月5日にマルウェア感染したことにあると判断しております。

(4) 二次被害又はそのおそれの有無及び内容

一部のお客様が配信メッセージに記載されたフィッシングサイトに対しクレジットカード情報の提供を行ってしまったとのご連絡を頂いておりますが、金銭的実被害の発生は確認できておりません。

3．お客様へのお願い

お客様におかれましては、疑わしいメッセージの配信を受けた場合、貼付されたURLリンクへのアクセスをされないようお願い申し上げます。心当たりの無い内容の場合はBooking.com社または下記弊社窓口へお問合せください。

本件に関するお問い合わせは、以下の窓口からお願いいたします。

【「モンタン博多」のご宿泊・予約のお客様窓口】

info@montan.jp

４．今後の対応と再発防止策

調査結果及び関係機関等からの指摘を踏まえ、セキュリティ対策ツールの追加導入や従業員に対する教育等、対策の強化を行ってまいります。

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

以上

モンタン博多

支配人

December 27, 2023

[Important Notice]
(Update)Apology and Notice Regarding the Possibility of Personal Information Leakage Due to Unauthorized Access to the Booking.com Management System and Delivery of Messages Leading to Phishing Sites

We deeply apologize for the severe inconvenience and concern we have caused our customers due to an unauthorized access to the Booking.com management system resulting in the potential leak of personal information. Regarding the "[Important Notice] Regarding unauthorized e-mails from Booking.com" published on October 6, 2023, we would like to report the facts as determined by subsequent investigations as follows.

October 6 Announcement:
【Montan Hakata】Announcement (montan.jp)

1. Chronology of the Incident

On October 5, 2023, we confirmed that an unauthorized access had been made within the Booking.com management system, and messages leading to phishing sites, etc., were delivered to some guests who had made a reservation at "Montan Hakata" through Booking.com. There is also a possibility that personal information of guests stored in the management system was viewed by a third party.
Since then, we have sent messages to guests who received the above messages to raise awareness, and we have also conducted ID and login password changes and computer security inspections at Montan Hakata.

2. Details of the Incident

(1) Number of Potentially Leaked Personal Information

Personal information of guests who have made reservations at "Montan Hakata" stored inside Booking.com management system, 680 cases.

(2) Details of Potentially Leaked Customer Personal Information

Name / Telephone Number / Email Address / Nationality

Credit card information and financial institution account information related to payment are not included.

(3) Source of the Breach

Following an in-depth investigation by cybersecurity experts, it was concluded that the incursion stemmed from malware that had infected two devices operated by “Montan Hakata” on October 5, 2023.

(4) Secondary Damage or Risk Thereof

We have been notified by a subset of our clientele that they may have inadvertently disclosed credit card information to the phishing sites mentioned in the dispatched messages. At present, we have not verified any financial harm arising from these incidents.

3. A Plea to Our Guests

We urge you to exercise caution and refrain from accessing any links embedded within messages of dubious origin. Should you encounter any unfamiliar content, please do not hesitate to reach out to Booking.com or directly to our customer service team as detailed below. Inquiries concerning this issue can be directed to:

【Customer Service for Accommodations and Reservations at Montan Hakata】

Email: info@montan.jp

4. Ongoing Measures and Prevention Efforts

With the insights gained from our investigation and the recommendations from the relevant authorities, we are committed to bolstering our defense measures, which include the deployment of advanced security tools and the provision of extensive staff training. Once again, we offer our deepest regrets for the distress and inconvenience this situation has caused.

Sincerely Yours,

montan HAKATA

Hotel Manager

2023년 12월 27일

[중요 공지]
(업데이트) Booking.com 관리 시스템에 대한 무단 접근 및 피싱 사이트로 안내하는 메시지 발송으로 인한 개인정보 유출 가능성에 대한 사과 및 공지

저희는 Booking.com 관리 시스템에 대한 무단 접근으로 인해 고객님들의 개인 정보가 유출될 가능성이 있어, 고객님들께 심각한 불편함과 걱정을 끼쳐드린 점에 대해 깊이 사과드립니다.

2023년 10월 6일에 발표된 "[중요 공지] Booking.com에서 보내는 부정 메일에 대해서"와 관련하여, 이후 조사를 통해 밝혀진 사실을 다음과 같이 보고드립니다.

2023년 10월 6일 공지:
【몬탄 하카타】공지사항 (montan.jp)

1. 사건의 경과
2023년 10월 5일, 저희는 Booking.com 관리 시스템 내부에서 무단 접근이 있었으며, "몬탄 하카타"에서 예약을 한 일부 고객들에게 피싱 사이트 등으로 안내하는 메시지가 발송되었다는 것을 확인했습니다. 또한 관리 시스템에 저장된 고객의 개인 정보가 제3자에 의해 열람될 가능성도 있습니다.
그 이후, 저희는 해당 메시지를 수신한 고객들에게 경각심을 일으키는 메시지를 발송하였고, 몬탄 하카타에서 ID 및 로그인 비밀번호 변경과 컴퓨터 보안 검사를 실시하였습니다.

2. 사건의 세부 사항
(1) 유출 가능성이 있는 개인 정보 수
Booking.com 관리 시스템 내에 저장된 "몬탄 하카타" 예약 고객의 개인 정보, 680건.

(2) 유출 가능성이 있는 고객 개인 정보의 세부 사항
성명 / 전화번호 / 이메일 주소 / 국적
*결제와 관련된 신용카드 정보 및 금융 기관 계좌 정보는 포함되어 있지 않습니다.

(3) 침해의 원인

사이버 보안 전문가의 심층 조사 결과, 2023년 10월 5일에 “몬탄 하카타”가 운영하는 두 대의 기기가 맬웨어에 감염되어 침해가 발생한 것으로 결론지었습니다.

(4) 2차 피해 또는 그 위험성

일부 고객으로부터 발송된 메시지에 언급된 피싱 사이트에 신용카드 정보를 실수로 제공했다는 통지를 받았습니다. 현재로서는 이러한 사건으로 인한 재정적 손실은 확인되지 않았습니다.

3. 고객님들께 드리는 부탁

의심스러운 출처의 메시지에 포함된 링크 접속을 자제해 주시기 바랍니다. 익숙하지 않은 내용을 접하시면, 주저하지 말고 Booking.com 또는 아래에 자세히 안내된 저희 고객 서비스 팀으로 연락해 주십시오. 이 문제에 관한 문의는 다음으로 해 주시기 바랍니다:

【몬탄 하카타 숙박 및 예약 고객 서비스】

이메일: info@montan.jp

4. 진행 중인 조치 및 예방 노력

조사 결과와 관련 기관의 권고를 바탕으로, 고급 보안 도구의 도입과 직원 교육 제공을 포함한 방어 조치를 강화할 것을 약속드립니다. 이 상황으로 인해 겪으신 불편함과 고통에 대해 다시 한번 깊은 사과의 말씀을 드립니다.

몬탄 하카타

호텔 매니저