[중요 공지(후속 조치)]

피싱 사이트로의 직접 메시지 전달에 대한 사과 및 통지

금번에, 호텔 르포르 코지마치가 이용하고 있는 Booking.com 사의 숙박 예약 정보 관리 시스템에 대해서, 악의를 가진 제 3 자에 의한 부정 접속으로, 관리시스템을 이용하여 당 호텔을 예약해주신 일부 고객님들에게 피싱 사이트로 유도하는 메시지가 발송된 건에 대해서, 고객님들께 불편과 우려를 끼쳐드린 부분에 대해 깊이 사과드립니다.

2024 년 6 월 12 일에 공지드린 "[중요 공지] 피싱 사이트로의 유도 메시지 발송에 따른 사과 및 공지]" 에 따라, 그 이후의 조사로 판명된 결과를 아래와 같이 보고드립니다.

(피싱 사이트란, 진짜 웹사이트인 것처럼 가장하여 부정한 수단으로 개인정보나 금융정보를 취득하려는 가짜 웹사이트를 말합니다.)

호텔 측은 관련 기관 및 Booking.com 사와 연계하여 원인 규명과 피해 상태 및 규모 조사를 진행하였습니다.

1. 조사 결과 (원인에 대하여)

그 결과, 이번에 관리 시스템에 부정 액세스를 당한 원인은, 가짜 관리 시스템의 로그인 화면에서 실제 사용 중인 ID 및 패스워드를 입력하여 정보가 탈취당해 무단 도용 된 것으로 확인되었습니다.

2. 조사 결과 (피해 현황에 대하여)

Booking.com 사의 조사 결과, 관리 시스템에 등록되어있는 고객님의 개인정보가 제 3 자에게 유출, 공개되었을 가능성은 없다는 보고를 받았습니다.

또한, 일부 고객님들에게 피싱 사이트로 유도하는 URL 링크가 첨부된 메시지가 발송된 후, 발송된 고객님들에게 주의를 요한다고 연락드렸습니다만, 이미 피싱사이트에 접속하여 카드번호 등을 입력해버리신 경우 등의 피해가 일부 있었음을 보고받았습니다.

고객님들께서는 의심스러운 메시지에 주의해 주시길 부탁드리며, 그러한 메시지를 수신받은 경우, 첨부된 URL 링크 등에 접속하지 않으시길 부탁드립니다.

3. 향후의 대응과 재발 방지 대책

이번 조사결과 및 관련 기관으로부터의 지적을 바탕으로, 이후 보안대책을 추가적으로 도입하고, 직원 교육을 강화하여 대책을 수립하겠습니다.

4. 문의처

본 건에 관련한 문의사항이 있으신 분은 Booking.com 고객지원팀 예약부서로 직접 연락 부탁드립니다.

+81-3-6837-0490 (예약 담당 부서는 1 번을 눌러주세요.)