UNION DES MÉTIERS ET DES INDUSTRIES DE L'HÔTELLERIE

Dossier Pratique n°18

Date : 13/10/2023

Hôteliers : vigilance – cyber attaque BOOKING

Nous vous informons régulièrement des tentatives d'arnaque sur les plateformes et notamment BOOKING. Une nouvelle attaque a de nouveau été signalée sur BOOKING. L'UMIH fait le point.

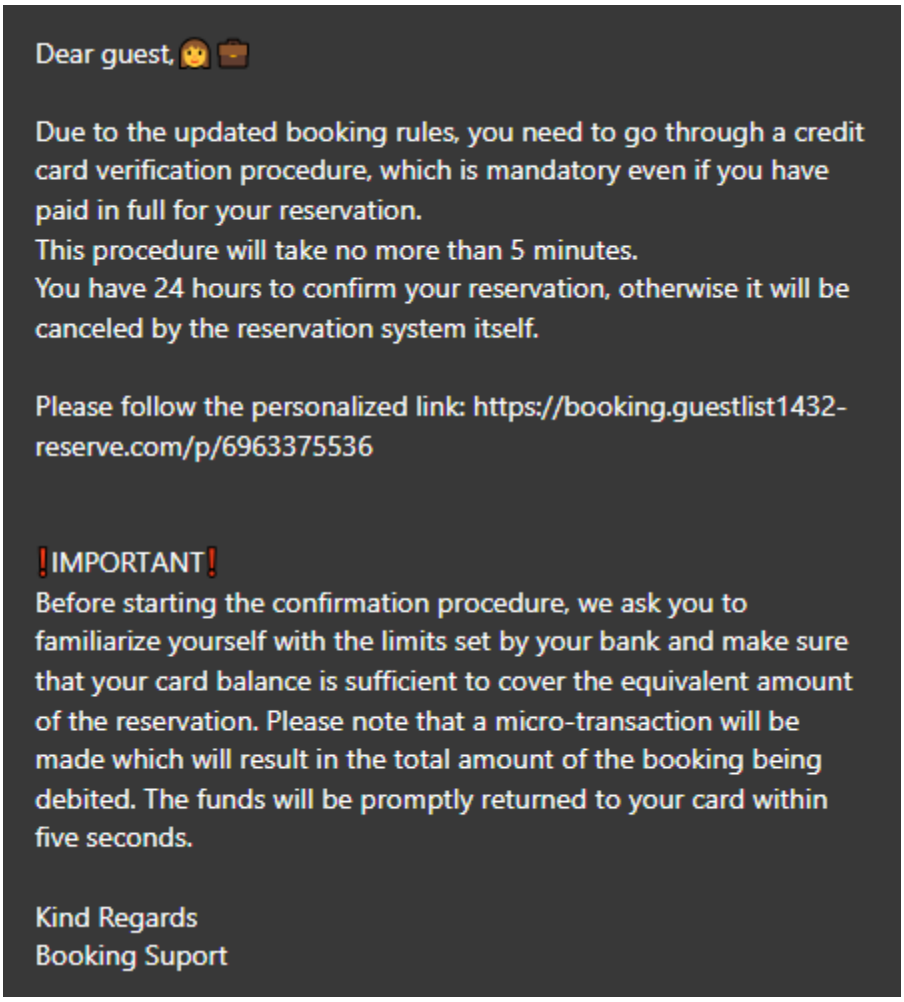
Le présent « Net hôteliers » vous informe d'une nouvelle attaque en ligne sur la plateforme BOOKING et vous informe des différents éléments d'identification et précautions à prendre.

1) De quoi s'agit-il ?

Les fraudeurs piratent l'extranet BOOKING des hôteliers et envoient des messages aux clients ayant fait des réservations dans leurs établissements en leur demandant de procéder à une vérification de leur moyen de paiement.

Les clients sont invités à cliquer sur un lien et se retrouvent à payer 2 fois le séjour !

Exemple de mail reçu par les clients :



Dear guest,👩💼

Due to the updated booking rules, you need to go through a credit card verification procedure, which is mandatory even if you have paid in full for your reservation.
This procedure will take no more than 5 minutes.
You have 24 hours to confirm your reservation, otherwise it will be canceled by the reservation system itself.

Please follow the personalized link: https://booking.guestlist1432-reserve.com/p/6963375536

❗IMPORTANT❗
Before starting the confirmation procedure, we ask you to familiarize yourself with the limits set by your bank and make sure that your card balance is sufficient to cover the equivalent amount of the reservation. Please note that a micro-transaction will be made which will result in the total amount of the booking being debited. The funds will be promptly returned to your card within five seconds.

Kind Regards
Booking Suport

2) Que faire ?

Pour vous prémunir, nous vous recommandons de vérifier qu'aucune activité anormale n'existe sur votre extranet Booking et d'effectuer les démarches minimales suivantes :

1. Mise à jour de vos antivirus
2. Changement du mot de passe du site Booking et changement du mot de passe de l'adresse email liée au compte Booking
3. Sensibiliser vos salariés
4. Prévenez tous les clients concernés
5. Faire un signalement à BOOKING : https://partner.booking.com/fr/aide/cadre-juridique-et-s%C3%A9curit%C3%A9/securite/signaler-un-probl%C3%A8me-de-s%C3%A9curit%C3%A9

De telles fraudes peuvent causer des dommages financiers substantiels et aussi porter directement préjudice à la réputation de l'hôtel.

Pour information, BOOKING se décharge de toute responsabilité et considère que la gestion de la fraude incombe aux hôteliers (clients mécontents, e-réputation, etc).
L'UMIH conteste la position de la plateforme et va adresser un courrier à BOOKING en ce sens et procéder à un signalement auprès des autorités françaises.

RESTEZ VIGILANT POUR PROTEGER VOTRE ACTIVITE

En restant vigilants et en prenant les précautions nécessaires, les hôteliers peuvent minimiser les **risques de cyberattaques** et protéger leur entreprise. Ne jamais sous-estimer les risques de la cybersécurité de prendre des mesures pour protéger les informations sensibles de l'hôtel est indispensable.

VOICI DES CONSEILS POUR GARANTIR LA SECURITE DES EXTRANETS DE L'HOTEL CONTRE LES CYBERATTAQUES :

1. **Soyez vigilant face aux tentatives de phishing** : ne cliquez jamais sur des liens douteux ou entrez des informations sensibles dans des formulaires en ligne non sécurisés. Si vous recevez un e-mail suspect qui semble provenir de Booking.com ou d'un OTA, le signaler à Booking.com ou à l'OTA pour qu'ils puissent prendre des mesures pour protéger les autres hôteliers ;
2. **Mettez à jour régulièrement les logiciels de cybersécurité** pour vous prémunir contre les logiciels malveillants ;
3. **Surveillez les réservations en temps réel** : vérifiez régulièrement les réservations pour détecter toute activité suspecte et prenez des mesures pour protéger l'hôtel contre les commandes frauduleuses ;
4. **Vérifiez régulièrement les paramètres de sécurité de l'extranet** : assurez-vous que ceux sont configurés de manière à protéger les informations sensibles de l'hôtel ;
5. **Formez les employés pour reconnaître les tentatives d'escroquerie** : informez vos employés sur les risques de cyberattaques et les techniques utilisées pour les détecter ;
6. **Employez des mots de passe sécurisés forts et uniques** pour tous les comptes liés à l'extranet de l'hôtel ;
7. **Utilisez des pare-feux et des logiciels antivirus** pour protéger l'extranet de l'hôtel contre les cyberattaques ;
8. **Recourez à une connexion sécurisée pour accéder à l'extranet de l'hôtel** et pour effectuer des réservations.
9. **Sauvegardez régulièrement les données de l'hôtel** : effectuez des sauvegardes régulières de toutes les données importantes de l'hôtel, telles que les informations de réservation et la base de données clients, pour pouvoir les restaurer en cas de cyberattaque ;
10. **Limitez l'accès à l'extranet de l'hôtel aux employés qui en ont absolument besoin** pour leur travail et mettre en place des procédures de vérification de l'identité ;
11. **Choisissez si possible une authentification à deux facteurs** (aussi appelée double authentification) pour renforcer la sécurité de l'accès à l'extranet de l'hôtel ;
12. **Suivez avec attention les activités en ligne de gestion de l'hôtel** tels que les réservations et les paiements, pour détecter toute activité suspecte ;
13. **Continuez à vous tenir informé sur les tendances de la cybersécurité** pour mieux protéger l'hôtel contre les cyberattaques.

QUE FAIRE EN CAS DE CYBER ATTAQUE ?

Contactez au plus vite la plateforme de l'Etat Cybermalveillance qui vous conseillera et vous indiquera les procédures à suivre à partir d'un diagnostic en ligne.

Portez plainte dans un commissariat de police ou un commissariat de gendarmerie pour fraudes informatiques (plus exactement "atteintes aux systèmes de traitement automatisé de données") en mentionnant les articles 323-1 à 323-7 du Code pénal.

Signalez dans les 72 heures suivant l'attaque la faille de sécurité à la CNIL en indiquant l'OTA comme partie impliquée via **le formulaire en ligne de violation de données personnelles**.

Prévenez les clients impliqués et les employés s'il y a une violation de données personnelles avec la cyberattaque.

S'il s'agit d'une attaque concernant un extranet lié à Booking.com : **contactez le service client** pour signaler un problème de sécurité (ou rentrez en contact avec l'OTA concerné).