Subject: Booking.com users targeted with scam messages [#377094355]

Booking.com users targeted with scam messages

Dear subscriber,

Those using the platform Booking.com to book their holidays or accommodation are being warned they could be targeted with emails or messages requesting payments from hotels who have had their account taken over by fraudsters. Between June 2023 and September 2024, Action Fraud received 532 reports from individuals, with a total of £370,000 lost.

Insight from Action Fraud reports suggests the individuals were defrauded after receiving unexpected messages and emails from a Booking.com account belonging to a hotel they had a reservation with, which had been taken over by a criminal. Using this account, the criminals send in-app messages, emails, and WhatsApp messages to customers, deceiving them into making payment and/or requesting credit card details.

The specific account takeovers are likely to be the result of a targeted phishing attack against the hotel or accommodation provider, and not Booking.com's backend system or infrastructure.

Adam Mercer, Deputy Head of Action Fraud, said:

"With more than 500 reports made to Action Fraud, those who have booked a holiday on the Booking.com platform should stay alert to any unexpected emails or messages from a hotel using the Booking.com platform, as their account could have been taken over by a criminal.

"If you receive an unexpected request from a hotel's account you booked with using Booking.com, asking for bank details or credit card details, it could be a fraudster trying to trick you into parting ways with your money. Contact Booking.com or the organisation directly if you're unsure.

"Remember to report any suspicious emails by forwarding it to report@phishing.gov.uk, or if you receive a fraudulent text message, you can forward it to 7726."

How can you protect yourself?

Booking.com and Action Fraud are providing the following advice on how to spot signs of fraud and protect your Booking.com account:

- No legitimate Booking.com transaction will ever require a customer to provide their credit card details by phone, email, or text message (including WhatsApp).
    - Sometimes a hotel provider will manage their own payment and may reach out to request payment information, like credit card details – before providing any information, always verify the authenticity of communication between yourself and the hotel's account.
- If you receive any urgent payment requests that require immediate attention, like a booking cancellation, immediately reach out to the Booking.com Customer Service team via the details on the official Booking.com website and/or app to confirm.
    - Any payment requests that do not match the information in the original booking confirmation should also be double checked and confirmed with Booking.com Customer Service before proceeding.
- Any messages purporting to be from Booking.com that contain instructions to follow links and/or open/download files should be treated with caution.
    - If you have any doubts about a message, contact Booking.com directly. Don't use the numbers or address in the suspicious message and use the details from their official website.
- For more information about how to protect your Booking.com account, please visit: Safety Tips for Travellers | Booking.com

If you receive any suspicious emails or text messages, report them by forwarding emails to: report@phishing.gov.uk, or texts to 7726.

Find out how to protect yourself from fraud: https://stopthinkfraud.campaign.gov.uk

If you've lost money or provided financial information as a result of any phishing scam, notify your bank immediately and report it to Action Fraud at https://www.actionfraud.police.uk/report-phishing or by calling 0300 123 2040. In Scotland, call Police Scotland on 101.

(If you found this information useful, please share it with friends, family and colleagues)

Message Sent By
Action Fraud
(Action Fraud, Administrator, National)

To reply or forward please use the below or these links: Reply, Rate, Forward / Share.

To login to your account click here, to report a fault click here, or unsubscribe

You are receiving this message because you are registered on Notts Alerts. Various organisations are licensed to send messages via this system, we call these organisations "Information Providers". Please note that this message was sent by Action Fraud (NFIB) and that Action Fraud (NFIB) does not necessarily represent the views of Notts Alerts or other Information Providers who may send you messages via this system.

You can instantly review the messages you receive and configure which Information Providers can see your information by clicking here, or you can unsubscribe completely, (you can also review our terms and conditions and Privacy Policy from these links).

This email communication makes use of a "Clear Image"(gif) to track results of the email campaign. If you wish to turn off this tracking for future emails, you can do so by not downloading the images in the e-mail itself. All links in the body of this email are shortened to allow click through monitoring.

VISAV Limited is the company which built and owns the Neighbourhood Alert platform that powers this system. VISAV's authorised staff can see your data and is registered with the Information Commissioner's Office as the national Data Controller for the entire database. VISAV needs to see your data in order to be able to manage the system and provide support; it cannot use it for commercial or promotional purposes unless you specifically opt-in to Membership benefits. Review the website terms.

Hide message history

E