

LexisNexis - Booking.com Product Security Partnership Overview

Protecting travelers and hotels through advanced risk solutions

Booking.com & LexisNexis Risk Solutions
April 2026

Account Security Partnership Overview

How Booking.com Account Security leverages LexisNexis Risk Solutions to protect customers and partners

handshakePartnership since
February 2024

Scope

- [check_circle](#)Account Takeover
- [check_circle](#)Fake Users
- [check_circle](#)Phishing

Contents

01 About Booking.com Product Security

02 The Threat Landscape and Challenges

03 Partnership: Why LexisNexis

04 Use Cases

05 Looking Ahead

Product & Account Security

Our Core Mission

To provide a secure and smooth experience for travellers and hotels - where customer trust is key and users feel safe using Booking.com.

se

cu

rit

User Protection

We protect users against account takeovers as well as fake registrations.

hu

b

Organizational Context

Part of the CyberSecurity function at Booking.com.

The Threat Landscape Context

hotel

Partner Account Takeover

Attackers compromise accommodation partner accounts to redirect payments, steal guest details, or conduct social engineering.

group
package
ad

Fake Guest Account Creation

Automated creation of synthetic traveller accounts for abuse of promotions, fake reviews, or inventory manipulation.

personal
contact
activity

Guest Account Takeover

Traveller accounts hijacked to redeem loyalty points, make fraudulent reservations, or conduct phishing.

email

Phishing

Compromised accounts used to send phishing messages via the platform, exploiting trust to target guests.

Current challenges

AI-Powered Phishing Attacks

AI-powered phishing attacks are rapidly evolving, targeting multiple with constantly changing tactics

Fake Traveller Accounts

Fake traveller accounts are created to deliver phishing and malware content to hotels or impact the hotel availability.

Compromised Hotel Messaging

Phishing messages are sent to travelers with active bookings from compromised hotels to collect payments or gain account access.

Malware & Account Takeover

Attackers are using malware to take over accounts and obtain access to the user rewards.

Our Collaboration with LexisNexis



Extensive Device Analytics

Profiling and machine learning signals. Covering both hotel and traveler user accounts.



Hotel Account Takeover Prevention

New prevention controls for hotel account takeovers.



Enhanced Malware Visibility

Higher visibility on malware attacks and dorm.



Faster Fake Sign-up Detection

New machine learning signals for a faster detection of fake sign-ups.

Use Cases:



Fake Guest Accounts Prevention

- LexisNexis signals at guest sign-up (web) identify device/network patterns consistent with automation, shared infrastructure, or known fraud networks.
- Inline prevention at registration reduces the volume of fake accounts requiring downstream remediation.



2FA Friction Reduction for Hotels

- Two-factor authentication is a key account takeover defence, but excessive 2FA challenges degrade the experience for legitimate hotels.
- LexisNexis device trust signals enable adaptive 2FA
- Reduce unnecessary 2FA verification costs while maintaining or improving security outcomes.
- Dual value: account takeover prevention AND customer experience improvements.

Looking Ahead



Extended Optimisation for App Traffic

Continuous improvement of LexisNexis models for mobile application environments.



LexisNexis Models Performance Benchmarking

Rigorous evaluation of false positive rate, true positive rate, and coverage across various attack types.



Collaboration with Fraud Teams

Close partnership to share insights and enhance overall fraud detection capabilities.



Regulatory and Privacy Alignment

Ensuring all integrations remain compliant with evolving global privacy requirements.

