High-Level Best Practice Guidelines for Connectivity Providers

Security and the protection of personal data is a top priority at Booking.com. As cybercriminals become more savvy, it's crucial to stay on top of emerging threats and make sure you can recognise the red flags of suspicious activity. Although actual incidents are rare – our dedicated teams leverage industry-leading technology to monitor, detect and block suspicious activity around the clock – we want to arm you with information and resources you need to stay safe on our platform.

To assist you in assessing the legitimacy of registration requests, we've put together a list of best practices you can follow to protect your platform. While these are by no means a substitute for robust internal security controls, they provide high-level guidance.

1. **Know who you are working with**
    - Consider verifying registration contact information, such as phone numbers and email addresses.
    - Consider verifying the address of the property.

2. **Monitor partner performance (*where applicable*)**
    - For partners with multiple registrations, we recommend that the performance of the connected properties is checked regularly to ensure that fraudulent partners are identified timeously.
    - Other partner performance indicators that could be considered are the volume of reservations and commission earned from the partner.

3. **Keep an eye out for abnormalities**
    - Abnormal partner behaviour, such as a lack of responsiveness, can be a red flag for suspicious activity.
    - Abnormalities in the volume of properties being listed for the region should be investigated.