Booking.com

Security Awareness for Partners

03

La sicurezza per i partner. Una guida per la consapevolezza

Sicurezza informatica

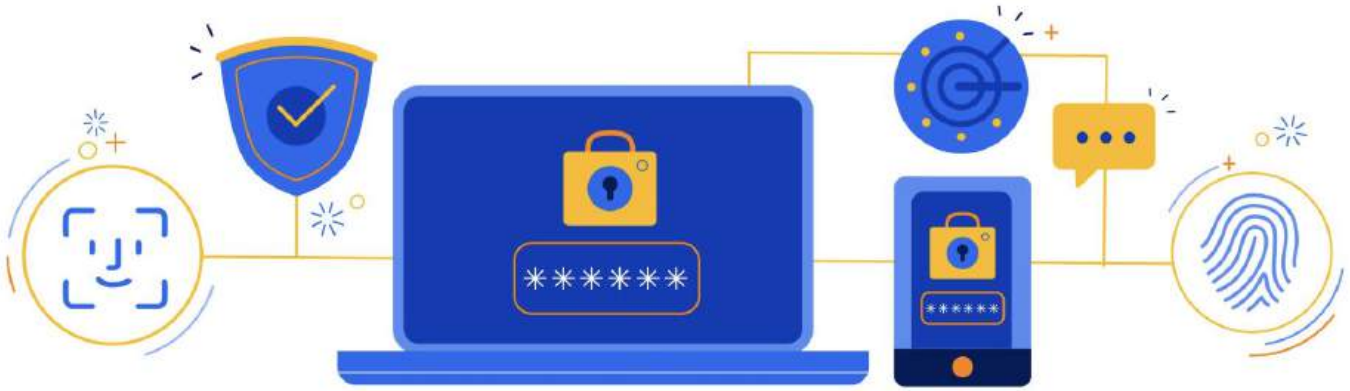
Aggiornamento: febbraio 2026

Booking.com

Argomenti trattati

All’interno di questa presentazione troverai:

- Un aggiornamento sulla sicurezza informatica e sulle minacce più comuni che affliggono il nostro settore
- Come identificare e contenere questi rischi nella tua azienda
- Cosa sta facendo Booking.com per prevenire gli attacchi e supportarti se ne subisci uno



Situazione attuale

Con l'evoluzione del nostro settore, le minacce alla sicurezza informatica e le tattiche adottate nei reati informatici sono diventate più sofisticate. È quindi più importante che mai restare vigili.

Un problema globale

In tutto il mondo e in tutti i settori, assistiamo a un costante aumento delle minacce informatiche, in linea con la tendenza degli ultimi anni.

Rischi in aumento

Man mano che il nostro settore continua a prosperare e a crescere, diventa un bersaglio sempre più allettante per i criminali informatici.

Collaborare per la sicurezza

È fondamentale lavorare insieme per creare un ambiente sicuro per i viaggiatori e per la tua attività.

Un supporto attivo

Continuiamo a potenziare le nostre misure di sicurezza online e forniamo indicazioni per aiutare i partner a rimanere al sicuro.

Le forme più comuni di frode informatica

Compromissione del sistema

L'accesso non autorizzato ai dispositivi avviene spesso tramite malware o software di controllo remoto.

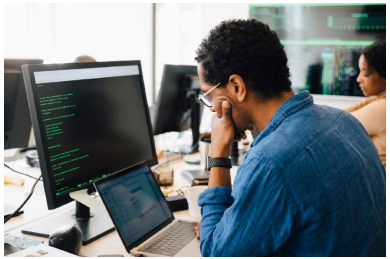
Può comportare il furto di identità, il furto di dati e l'hacking dell'account.

Solo un software antivirus può rilevare efficacemente gli attacchi di malware.

Hacking dell'account

Spesso è il risultato di un attacco di phishing, che comporta l'accesso non autorizzato e illegale a un account extranet.

Ciò può dare luogo a transazioni fraudolente e all'accesso non autorizzato ai dati degli ospiti negli account compromessi dei partner.

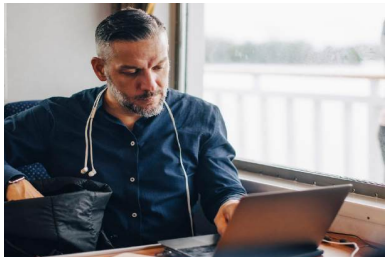


Prenotazioni fraudolente

Sono prenotazioni effettuate al solo scopo di sfruttare i vantaggi di marketing, senza che ci sia l'intenzione di soggiornare o pagare.

Danneggiano economicamente il partner, perché la disponibilità resta bloccata inutilmente e all'ultimo minuto il "cliente" cancella.

Le prenotazioni fraudolente possono essere sfruttate come strumento di ingegneria sociale e, in ultima analisi, portare all'hacking dell'account.



Violazioni esterne

Le violazioni esterne si riferiscono a incidenti in cui sistemi o servizi di terze parti che si collegano a Booking.com sono compromessi.

Ciò può dare luogo a transazioni fraudolente e all'accesso non autorizzato ai dati degli ospiti negli account compromessi dei partner.

Le nostre iniziative per migliorare le misure di sicurezza informatica

Abbiamo intensificato i nostri sforzi in materia di sicurezza informatica per garantire che ogni esperienza di prenotazione sia sicura, protetta e affidabile, per i nostri partner e viaggiatori.

I criminali informatici affinano i loro metodi, ma noi miglioriamo costantemente le nostre misure di sicurezza per affrontare queste sfide in modo tempestivo e proattivo.

Comprendiamo le difficoltà che potresti incontrare a causa di queste minacce.

Ma non preoccuparti: ci stiamo impegnando al massimo per potenziare le nostre misure di sicurezza e, unendo le nostre forze, possiamo avere la meglio su questi attacchi.

Le nostre iniziative per proteggere te e la tua attività

Protezione dell'extranet e sicurezza della messaggistica con i viaggiatori

- **Limitazioni alla modifica dei template**: per preservare l'integrità della comunicazione, solo gli account amministratore possono modificare i template dei messaggi nell'extranet.
- **Elenco degli URL e degli indirizzi e-mail consentiti**: questo elenco, gestito direttamente dai partner, protegge da link dannosi e mittenti non autorizzati.
- **Elenco dei domini bloccati**: ora gestiamo un elenco di domini il cui accesso è limitato per motivi di sicurezza, riducendo al minimo la probabilità di frode.
- **Rilevamento del phishing**: abbiamo implementato ulteriori algoritmi di apprendimento automatico per identificare e rimuovere i messaggi di phishing dai canali di comunicazione partner-ospite.

Maggiori informazioni sulle impostazioni di sicurezza della funzione di messaggistica sono disponibili nel Partner Hub.

Rafforzamento della sicurezza dell'account extranet e Pulse

- **Autenticazione basata sul rischio**: maggiore sicurezza e migliore esperienza dell'utente con l'autenticazione a due fattori attivata in base agli indicatori di rischio. Le verifiche si attivano solo quando vengono rilevati comportamenti sospetti, in modo da non disturbare i clienti veri.
- **Gestione delle attività dell'account**: per evitare usi impropri, gli account rimasti inattivi per 24 mesi vengono bloccati e dopo 24 mesi vengono proprio disabilitati.
- **Monitoraggio avanzato dei dispositivi**: un monitoraggio migliorato rileva in anticipo potenziali furti di credenziali e blocca gli account compromessi in modo più efficace.

Le nostre iniziative per proteggere te e la tua attività

Prevenzione delle frodi

- **Rilevamento più efficace delle false prenotazioni**: la nostra infrastruttura di sicurezza avanzata e gli algoritmi di apprendimento automatico identificano e bloccano rapidamente le prenotazioni sospette.
- **Capacità del supporto potenziata**: automazione migliorata per una gestione più rapida delle segnalazioni di prenotazioni fraudolente.

Aggiornamenti costanti

- **Guida alla sicurezza informatica**: una risorsa che ti aiuta a identificare i rischi e a salvaguardare i dati della tua attività e dei viaggiatori.
- **Video informativo su YouTube:** "Proteggere la tua attività dalle minacce online".
- **Contenuti del Partner Hub**: abbiamo una serie di contenuti informativi da esplorare.
- **Checklist delle migliori pratiche**: esamina la nostra checklist alla sezione "prevenire" attivamente le frodi di questa presentazione.

Supporto e tempi di risposta in miglioramento

- **Supporto più veloce**: ricevi supporto tempestivo per le attività di recupero dell'account e reimpostazione della password in caso di compromissione dell'account.
- **Formazione extra ai nostri dipendenti**: stiamo offrendo a tutti i dipendenti che ricoprono ruoli a contatto con i partner un training aggiuntivo su come supportarli al meglio con la prevenzione, il rilevamento e la risoluzione.

Il tuo ruolo nella sicurezza informatica

È essenziale **lavorare insieme** per ridurre l'impatto di questa problematica e garantire un ambiente sicuro, sia per i viaggiatori sia per la tua attività.

Ecco cosa puoi fare per rafforzare anche tu con noi la **sicurezza informatica**.

Segui gli aggiornamenti

Utilizza i contenuti di sensibilizzazione alla sicurezza forniti per tenerti al corrente delle minacce più recenti.

Scopri il nostro impegno per la sicurezza informatica

Identifica le attività sospette

Rimani sempre vigile contro i rischi informatici imparando a riconoscere i segnali a cui prestare attenzione.

Previeni le frodi prima che si verifichino

Utilizza le misure di sicurezza e le risorse fornite da Booking.com. Fai attenzione ai messaggi di phishing.

Gestisci correttamente le attività sospette

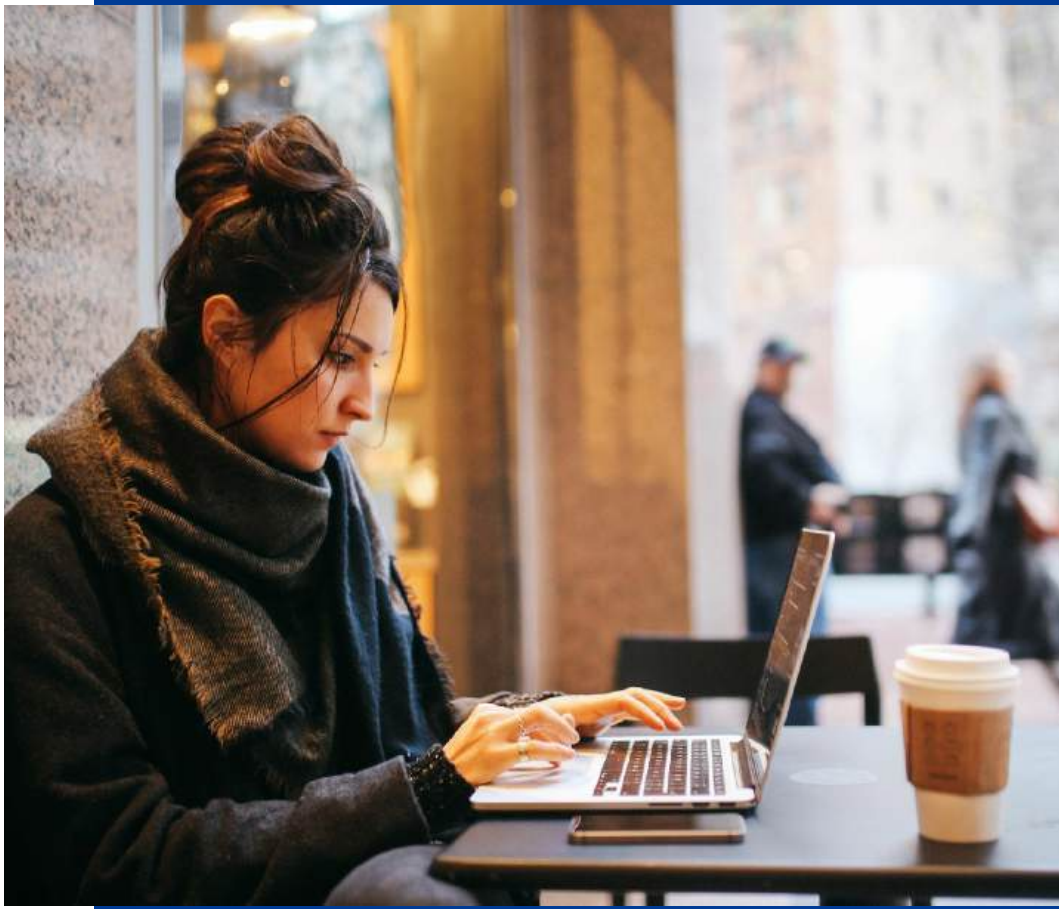
Segnala immediatamente qualsiasi attività sospetta e contribuisci alla sicurezza dell'intera community di Booking.com.

1. Identificare

Compromissione del partner

Segnali di attività sospette a cui prestare attenzione:

- Richieste sospette o urgenti di contatto diretto ricevute tramite chat o funzione di messaggistica degli ospiti.
- E-mail o messaggi di chat inviati direttamente a te, firmati “Booking.com”, che richiedono azioni urgenti da intraprendere o allegati da scaricare.
- E-mail o messaggi di chat che richiedono di copiare/incollare comandi e URL o di premere combinazioni di tasti sospette.
- Prenotazioni che includono una carta di credito non valida associata a una politica “Senza pagamento anticipato”.
- Chiamate di qualcuno che si spaccia per Booking.com e richiede credenziali di accesso (per es. nome utente, password, autenticazione a due fattori, ecc.) al tuo account extranet e Pulse o ad applicazioni di terze parti.

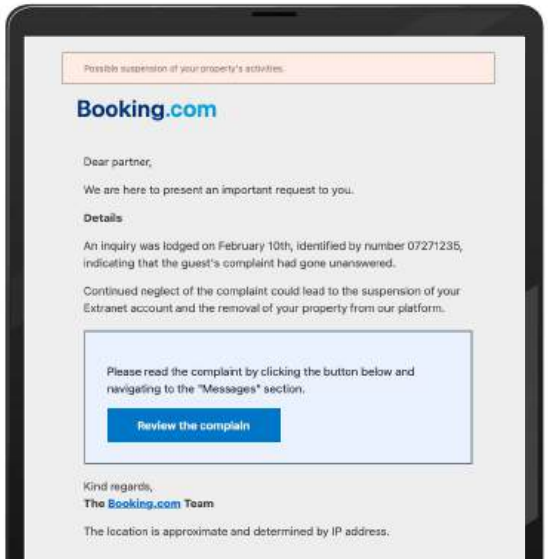


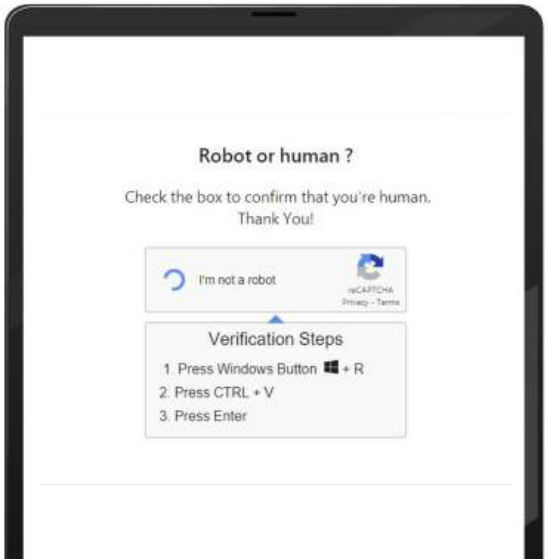
Hacking dell'account

Spesso vengono inviati messaggi di phishing tramite la casella delle richieste speciali o la chat (funzione di messaggistica) utilizzando come pretesto una prenotazione falsa. Ti viene quindi chiesto un contatto fuori piattaforma a cui gli hacker possono inviare malware da installare senza che i controlli di Booking.com riescano a intercettarlo.

I partner possono anche ricevere e-mail di phishing contenenti un dominio non vero e/o annunci di ricerca falsi che sembrano una pagina di accesso di Booking.com o di un altro sito. L'intento di questi messaggi è acquisire le tue credenziali al fine di compromettere i tuoi account **o indurti con l'inganno a scaricare software dannoso sul tuo dispositivo.** In questo modo, i malintenzionati possono raccogliere i dati identificativi dei clienti e reindirizzare i pagamenti a proprio favore.

Esempi tratti da casi reali

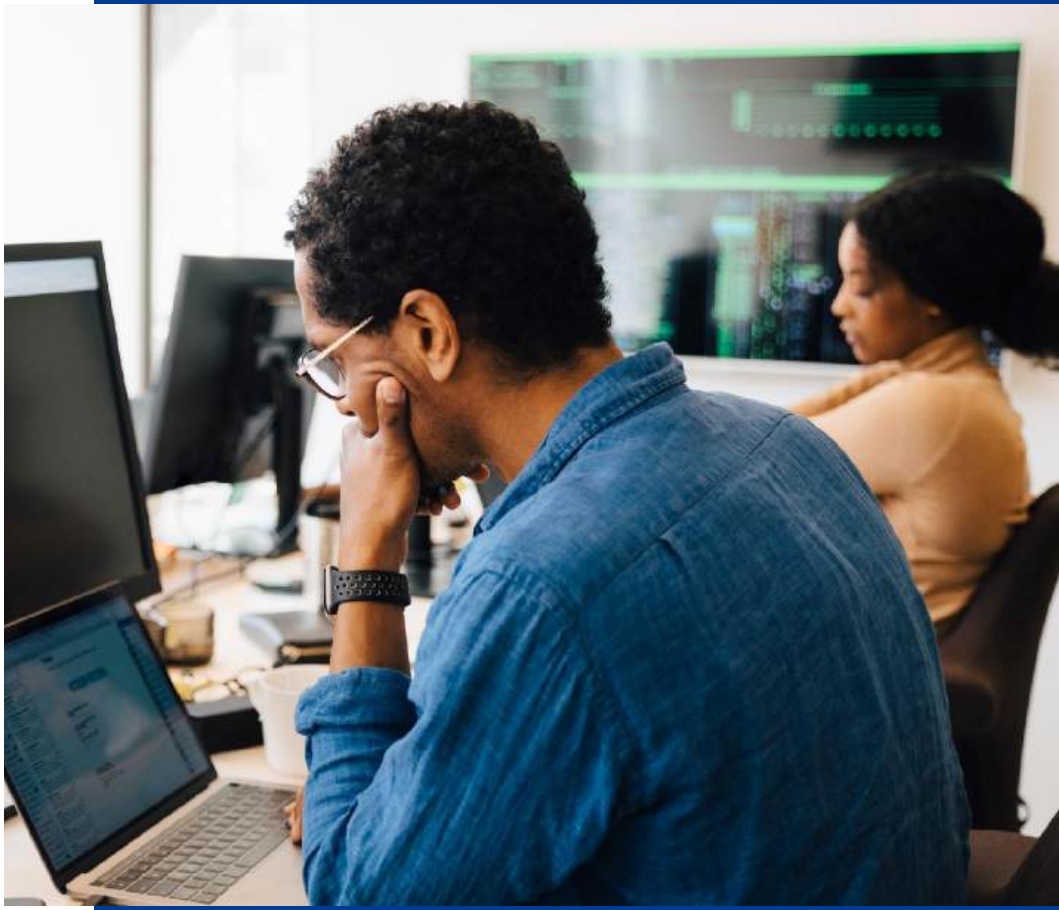




Prenotazioni fraudolente

Campanelli d'allarme di false prenotazioni a cui fare attenzione

- Prefissi o nomi insensati o nomi di personaggi famosi
- Prenotazioni con un numero insolitamente elevato di camere o prenotazioni multiple nello stesso hotel
- Più prenotazioni effettuate in rapida successione (per es. alle 14:05, 14:05, 14:05, 14:06, 14:06, 14:07 ecc.)
- Prenotazioni con una durata di soggiorno insolitamente alta
- Qualsiasi elemento descritto qui sopra combinato con prenotazioni last minute di alto valore
- Tentativo di prenotazione con carta di credito non valida
- Modifiche apportate subito dopo la prenotazione stessa
- Link inviati da un ospite (phishing)
- Tentativo da parte di un ospite di spostare la comunicazione fuori dalle piattaforme di Booking.com



2. Prevenire

Prevenire la compromissione del sistema e il furto di account

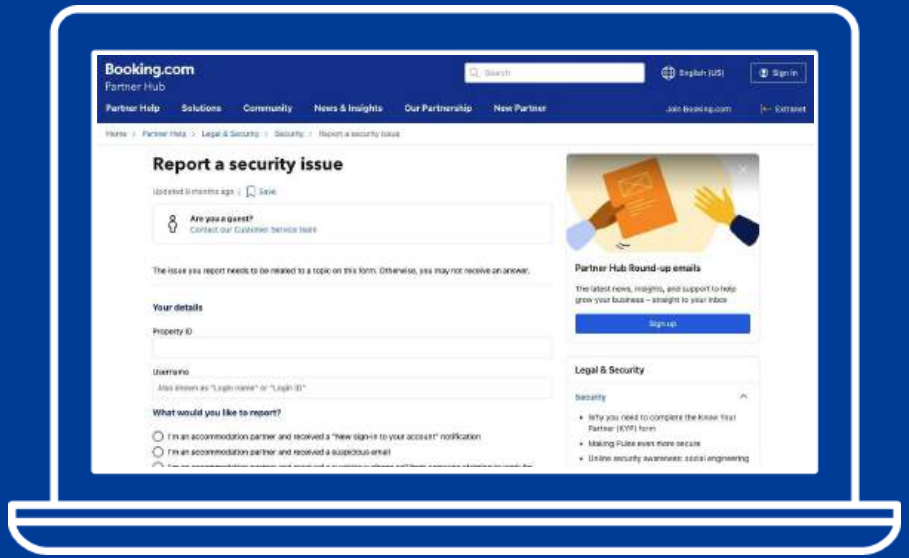
- Mantieni **aggiornati sistema e software**, **applica le patch di sicurezza** tempestivamente e **utilizza software antivirus**.
- Scopri di più sul phishing e su come riconoscerlo. Assicurati che le tue **protezioni dell'e-mail**, come i filtri antispam e il rilevamento degli URL dannosi, siano aggiornate e abilitate.
- Scarica e installa app solo da **fonti attendibili**.
- Utilizza sempre **password o passphrase complesse** e non riutilizzare né condividere le password.
- Imposta l'**autenticazione a due fattori** (2FA) su ogni piattaforma che utilizzi, come ad esempio la posta elettronica.
- Crea **account extranet individuali** per te e i tuoi dipendenti.
- **Rivedi i diritti** periodicamente e assicurati che sia concesso solo l'accesso minimo richiesto.
- Comunica sempre attraverso la **piattaforma di Booking.com**.
- Presta **particolare attenzione** ai messaggi con richieste strane o inaspettate, richieste urgenti che sottolineano la necessità di intraprendere azioni immediate, talvolta da parte di un'autorità o accompagnate da incentivi, o affermazioni relative a cambiamenti improvvisi in processi o circostanze eccezionali.
- **Non utilizzare l'account amministratore dell'extranet per le operazioni quotidiane**.

Prevenire le prenotazioni fraudolente

- Pre-autorizza la carta di credito dell'ospite collegata alla prenotazione, in base alle condizioni che hai impostato per la tua struttura.
- Segnala le carte di credito non valide tramite l'extranet. Se hai attivato i Pagamenti tramite Booking.com, ce ne occuperemo noi.
- Assicurati che la carta di credito utilizzata per l'addebito sia presentata all'arrivo, poiché eventuali incongruenze potrebbero indicare una potenziale frode.
- Assicurati che lo stato della prenotazione sia aggiornato correttamente e in modo tempestivo (per es. segnala eventuali mancati arrivi).
- Monitora attentamente attività sospette e insolite, come i segnali elencati sopra.

Considera la possibilità di intraprendere le seguenti azioni:

- Imposta i requisiti degli ospiti per le prenotazioni
- Aggiungi condizioni e penali di cancellazione
- Definisci i requisiti per il pagamento anticipato
- Imposta restrizioni alle prenotazioni per la tua struttura
- Segui i nostri consigli su come gestire le cancellazioni



Suggerimenti utili

- Segnala subito qualsiasi attività sospetta a:

  report.booking.com

- Attiva un programma antivirus e anti-malware sul tuo computer o sulla rete internet.
- Cancella i cookie nel browser che usi per accedere al tuo account extranet.
- Reimposta la password dei tuoi account Booking.com, dell'e-mail e di qualsiasi altro account di terze parti collegato.
- Controlla eventuali variazioni nel tuo account, come recapiti, dati contabili, tariffe e disponibilità, template messaggi, foto, ecc.

Ci impegniamo ad aggiornarti costantemente sulle nuove iniziative di sicurezza.

La nostra partnership si rafforza quando lavoriamo insieme per creare un ambiente online più sicuro, permettendoti di concentrarti con più fiducia sulla crescita della tua attività.