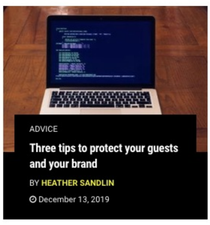
TRENDING COMMENT


ADVICE
Three tips to protect your guests and your brand
BY HEATHER SANDLIN
December 13, 2019


ADVICE
Securing guest data – the ongoing efforts of GDPR
BY HEATHER SANDLIN
December 12, 2019

Home › Features › Advice

Three tips to protect your guests and your brand

James Slatter explains why and how you should make your hotel security a high priority

December 13, 2019 *in* **Advice**, **Features**

Email Whatsapp Tweet Post

When guests arrive on property, security should be the last thing on their minds. Business and leisure travellers expect a secure stay experience with responsive service. However, as the industry has become an attractive target for fraudsters, hotels and resorts should make security a high priority.

How do hoteliers ensure that their property provides as secure an environment as possible, while maintaining high service standards? It is necessary to regularly evaluate data security programmes. This article outlines three tips for a proactive approach to minimising risk, as well as preventative actions to consider.

Monitor Loyalty Account Use

Perhaps surprisingly, loyalty account takeover is a growing challenge as fraudsters know that reward redemptions are not typically scrutinised as rigorously as traditional payment transactions. Your most loyal guests often accumulate high reward balances, making their reward points vulnerable to exploits.

Preventative Actions

Keep an eye out for account misuse. Train staff to recognise out-of-character guest behaviours. For example, members reported that fraudsters have spent loyalty points on luxury stays in cities where the members do not customarily travel. Large point redemptions in a single transaction should be scrutinised more closely.

You can also adjust your loyalty redemption process to align with the security protocols of your traditional payment transactions. Implementing a more stringent redemption process that requires the member to authenticate their account, such as providing personal identification, can help minimise upsetting your most loyal customers.

Safeguard Against Data Breaches

No matter how small, any breach is unfavourable. Breached data can negatively impact your business in terms of brand reputation and revenue loss. In some property management, point-of-sale and other systems that are used to process credit cards, the CV (Card Verification) numbers may be logged, making them accessible with minimal access by fraudsters.

Preventative Actions

Work with reliable property management solution (PMS) partners and a payment processing system that allows you to collect payments using the most up-to-date security standards. Look for technologies – or integrate to those that employ tokenisation. Verify that all your technology partners are PA-DSS, PCI-validated providers where applicable. Vulnerability scanning is another important measure that helps protect your data. If you have recently added or updated your PMS technology, booking engine, accounting system, sales and catering system, or any other systems that contain guest and finance data, it is time to perform a vulnerability scan.

Breakdown the Departmental Walls

IT and Security teams ideally should work hand-in-hand when it comes to protecting your business. Without a collaborative approach, it is difficult to know where you might have security gaps. Each area plays an important role in protecting business environments. IT focuses on delivering a scalable, flexible solution architecture to ensure you can run your business effectively, while Security focuses on cyber and network security, as well as on controlling access to physical areas.

Preventative Actions

Each department is equally critical for effectively deploying and maintaining the most up-to-date and secure business protocols. Make it a priority to foster interdepartmental relationships by placing the two departments under the same reporting structure. Alternatively, consider conducting regular interdepartmental security meetings in order to maintain open collaboration.

As the adage goes, "The best defence is a good offence." When it comes to data security, while these tips provide a good starting point, it is crucial to your business standing to have official documentation that outlines standard security policies and procedures to which staff will consistently adhere.

Additionally, continue to refresh and update your security policies to align with the latest protocols available in the market, and from your technology partners. In today's business landscape, preserving hospitality while protecting guests is the name of the game.

By James Slatter, managing director EMEA, Agilysys

The SME Files


The latest business data is bad news, but the reasons given spell a good omen
December 16, 2019

The election is over – time for the Tories to deliver for small businesses December 13, 2019

Businesses are sitting on £115bn and waiting to splurge December 12, 2019

Small business owners dip into personal wealth to survive? Of course they do December 11, 2019

LATEST NEWS


Cycas Hospitality names Peter Habelitz as new CFO
December 16, 2019


Harrington Hall Hotel acquired in joint venture
December 16, 2019


New government must 'fulfill election promises' to businesses, says UKH
December 16, 2019


Hilton Hotel Sheffield closes after 20 years
December 16, 2019


The election is over – time for the Tories to deliver for small businesses
December 13, 2019