Published on *The National Law Review* https://natlawreview.com

67% of Hotel Websites Expose Guest Data, Study Finds

Article By:

Risk Management Magazine

According to new research from cybersecurity company Symantec, 67% of hotel websites are leaking customer reservation details and other personal information. Candid Wueest, the company's principal threat researcher, tested more than 1,500 hotels in 54 countries, including low-cost to high-cost hotels, as well as both chain and independent hotels.

HOTEL BOOKINGS AND PRIVACY

How Your Private Data could be Compromised

After you book a hotel online, you usually get an email confirmation. The email contains a convenient link to allow you to view and manage your booking—often without needing further authentication. This practice poses a significant risk to your privacy.

CONFIRMATION EMAIL

1 BOOKING SYSTEM

The user makes an online booking and receives a confirmation email containing a direct access URL.

2 USER

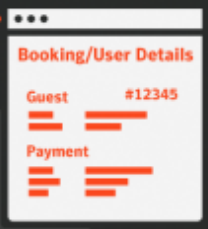
The user clicks on the direct access URL to view their booking details.

of confirmation emails include a direct access URL to view booking details (no authentication required)

of confirmation emails that contain a direct access URL also use insecure URLs which are vulnerable to traffic sniffing

http://hotel.tld/?login=12345

HOTEL WEBSITE



https://analytics.tld/?referrer =http://hotel.tld/?login=12345

ANALYTICS

3 ANALYTICS PROVIDERS

The booking website incorporates third-party analytics components, which are loaded by making requests to third-party servers. These requests are done behind the scenes via HTTPS but the full referrer URL (the direct access URL) is passed to the third party in the process.

4 INSIDER

A malicious insider at the third party could use these referrer URLs to access the booking management page as if they were the user. This could expose private information and also allow the insider to modify or even cancel bookings.

http://hotel.tld/?login=12345

Symantec.

When a customer uses a hotel's website to book a room, the site usually creates and sends them a link so that the customer can directly access and manage their reservation. According to Symantec, part of the problem is that third-party advertisers on hotels' booking websites and web analytics companies (which track web traffic) can access customers' bookings because they also get those links. This means that advertisers and analytic companies – including any potential malicious actors among their employees – could access and steal the information that the customer entered when booking a room, and even change or cancel the reservation.

Symantec also found that more than a quarter of the hotel websites examined do not send secure, encrypted links in their confirmation emails. Encrypted links prevent anyone trying to hijack a customer's data from being able to see that data. If a customer received a confirmation email while using an unprotected WiFi (a public network in a café or an airport, for example), a cybercriminal could intercept that customer's emails and use the unencrypted hotel booking link to access the customer's booking. Some of these automatically generated links also contain details like customers' email addresses in the web address, which makes accessing their information even easier for cybercriminals.

Additionally, many hotel websites are vulnerable to a type of cyberattack called "brute forcing," where an attacker can use the customer's email address and guess their booking number to gain access to the reservation and personal information. In some cases, Symantec found that hotel websites did not even require an email address to access customers' reservation information via brute forcing. Though this method would not be useful to gain access to large amounts of customer data, attackers could use it to target individuals, like a specific CEO or conference attendee.

Wueest noted that hotels have thus far been slow to respond to these data exposure risks, and some have not responded at all. When he alerted the hotels' data privacy officers to the problems in their sites, 75% responded, and those who did took an average of 10 days. Hotels and their information security staff should promptly assess their booking processes to ensure they are minimizing the risk of potential data leaks and breaches. By leaving these gaps in their websites' security, they are endangering their customers and opening themselves up to risk, including potential liabilities and reputational damage.

Symantec recommends that hotels use encrypted links, and ensure that the automatic links generated do not include information like customers' email addresses. It also recommends that customers use Virtual Private Networks (VPNs, services that protects users' internet traffic) when booking or accessing their reservations using public WiFi to prevent any cyberattacker from intercepting any information that would provide a way in.

The report should also serve as a reminder that corporate employees' personal devices and personal information are popular targets for cybercriminals and can be especially vulnerable to risks while traveling. Any time an employee exposes their devices to unprotected networks or, in this case, insufficiently protected websites, it leaves both the employee and their employer at risk. Even if an employee is using their own device to conduct business, it still endangers their employer because it may expose valuable business information. Cybercriminals have particularly used the hospitality industry as a hunting ground for such attacks, for example, targeting individuals using hotel WiFi, tricking them into downloading malicious software and stealing their information or spying on their internet activity.

Authored by Adam Jacobson

National Law Review, Volume IX, Number 107