Crazy Things You Wouldn’t See in a Hotel
“Personal information posted on the wall”

We have all turned to digital commerce as a lifeline during the lockdown. As crazy as the pandemic has been, it is good to make light of crazier things that should not happen. The Media Trust and RH-ISAC are exploring some of those things in this series, *Crazy Things That Happen in your Online Store Every Day*.

Crazy Things #5 – Loyalty Data Exposed

Customer loyalty data for all to see.

We love loyalty programs and use them for everyday items: credit card purchases, gas stations, grocery shopping, travel, retail shopping, food shopping and yes, hotel stays! We often recommend loyalty programs to our friends and families, especially those who are avid collectors of loyalty points in search of free stuff. So, when your niece started traveling for work, naturally you recommended she sign up for the hotel’s loyalty rewards program; she might as well earn some perks while traveling. She did and filled in the requested personal information—from her birthday to room preference.

Imagine her horror one day when she found out that “someone from the hotel” had posted her registration information on the bulletin board in the lobby for all visitors to see. Furthermore, she could see the detailed histories of other members: where they stayed, when they stayed, their loyalty status, and more.

While she is loyal to the hotel, the hotel does not return that loyalty by safeguarding her information!

Seems crazy, right? But this happens on many hotel websites!

Guest loyalty program data is stolen by bad actors and sold to the highest bidders on the dark web, causing harm to both the hotel’s customers as well as significant damage to the hotel’s reputation. The data is exfiltrated by hijacking the loyalty program form using one of two methods:

Transparent overlay: The malicious code inserts a transparent overlay on the data input form to directly capture all entered data. Once the guest hits submit, all personal information is sent directly to the bad actor, and an error message occurs since the hotel website did not receive the necessary information. Often the guest will not suspect anything and re-enter the information.

Malicious code in the background: “Listening” in the background, the malicious code records the information being entered in the loyalty program form. When the guest hits submit, the hotel receives the information and registers her for the loyalty program. However, the bad actor also has a copy of the guest’s data!

Overcoming crazy isn't an insurmountable feat.

For 15 years we have been helping companies with deep 24x7, 365 monitoring of their websites to detect malware and inventory every third-party vendor on their ecosystem. We establish what each vendor is doing and evaluate all data collection activity on your website to assess unauthorized data exfiltration.

Find out best practices in monitoring and what is happening on your website.

FIND OUT!

THE MEDIA TRUST
We know digital security.