

Crazy Things You Wouldn't See in a Retail Store

"Everybody knows your name"



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 #6 – Customer Data Privacy

Store associates know your personal information.

You walk into a mega-store, where you love to shop because they have such a wide range of products which fit your style and budget. A friendly store associate welcomes you to the store and asks you:

1. Did you enjoy your eggs and bacon this morning? You had stopped at a popular breakfast restaurant down the street before coming to the store. Strange...you have never met this associate, yet he appears to know you, where you were for breakfast, and what you ate.
2. He then inquires about your three-month-old niece, and whether the new diapers were helping her sleep better at night. How would he know about your niece??
3. Finally, he asks if your visit to Florida to see your parents this weekend went well, and if you enjoyed that hip new hotel during your visit. He then points to a section of the store, suggesting you check out some comfort shoes for your parents.

This is getting creepy! You have never met this store associate, yet he seems to know everything about you and where you had been recently...how is that possible?

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

Most companies do not know the vast amounts of customer data which can be harvested from their sites without their permission. Unauthorized data exfiltration is a significant digital risk, not only because it violates consumer data privacy, but also because data is an important company asset, and data loss is quantifiable financially. Protecting the privacy of your website visitors is critical to maintaining customer trust and your brand reputation. Data protection requires:

- **Continuous monitoring of data collection** activities across your site, especially your sensitive pages such as cart and checkout.
- **Continuous monitoring of data exfiltration activities** -- what is collected, how it is collected and what entity is performing the collection.
- **Create agreements and policies** with your third parties that addresses the governance of data collected on your website and mobile app.

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!

