Crazy Things You Wouldn’t See in a Retail Store

“Offering adult products to a child”

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 #7 – Regulatory Compliance Violations

Your 6-year-old is invited to the bar across town.

Your 6-year-old daughter has a new tablet for online schooling since her elementary school has shifted to meeting virtually. She also uses the tablet for watching cartoons, the occasional movie you have pre-approved, and a site with educational games her teacher recommended. You have limited access to only these sites, opted out of all online tracking and filled in her online profile, making it clear she is a child...after all, you can’t be too careful!

The next week your child starts to receive mail for all sorts of things, including the new bar opening nearby, a $50 coupon for a casino across town, and 30 percent off birth control pills. This is crazy...who would send mail like this to a 6-year-old? Now you can’t let your daughter near the mailbox.

Seems horrifying, right? In the digital world of eCommerce this isn’t just frightening, it is a violation of regulatory compliance.

Seems crazy, but this could happen on your online ordering websites!

There are a number of states and countries that have implemented regulations governing how retailers manage the privacy of their online customers. Those laws include the Children’s Online Privacy Protection Rule (“COPPA”), the California Consumer Privacy Act (“CCPA”), and the French Data Protection Authority’s (“CNIL”) guidelines on the use of cookies and similar technologies. Retailers seeking to avoiding violations that lead to fines and brand damage should implement:

Reasonable security practices - CCPA requires that retailers implement “reasonable security procedures and practices” to avoid breaches that lead to the theft of a consumer’s private information. Avoiding malware breaches of site visitor data is important, especially if that breach impacts a large number of visitors over an extended period of time.

Cookie opt-out validation - Retailers with customers located in California and France should implement systems to block the tracking of data if that consumer has opted out of tracking, or in the case of France, if those cookies track data for more than a year. To be certain that they are in compliance, retailers need to validate that opted out consumers are not being tracked.

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.