Crazy Things You Wouldn’t See in Curbside Pickup
“Competitors raid your drive-up line”

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 #4 – Customer Hijacking

Competitors steal your shoppers from the checkout line.

Your supermarket introduced a curbside food pickup service and has worked diligently marketing it to create steady customer growth over the last two years. Then the pandemic hit, and you started noticing a slow decline in your customers. At first, you didn’t think much of the seemingly innocent looking high school students who were handing fliers to customers as they pulled up to get their groceries. Then you noticed some of your customers would receive the fliers, turn around and leave without picking up their order. Why would they leave without picking up their groceries…what was going on?

You didn’t realize it then, but your customers were being hijacked. This happens EVERY minute in digital stores across the world.

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

Customer hijacking is common and affects all online commerce from restaurants to hotels. Hijacking is delivered through malware or unauthorized code injected—usually an advertisement—into the customer shopping experience to redirect customers away from your site. The customer journey is disrupted, and the customer is now purchasing from a competitor or a site with illegitimate products.

The impact of customer hijacking can be permanent if your competitors offer the value/price customers are looking for. And if enough of your customers are hijacked, it can damage your financial health. You can reverse the customer hijacking trend:

1. Scan all ads running on your site for malware, including JavaScript.
2. Flag and remove all retargeting ads, pop ups, redirects, non-secure cookies, and cookies without a strict SameSite attribute.
3. Scan your site with different profiles using various gender, geography, device type and OS/browser combinations. Customer hijacking is usually targeted, so you want to ensure you can replicate your customer experience.
4. Continuously monitor your website for third parties and their activities. Know who is on your site, who is collecting what information and how that impacts your customer experience.

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.