Bots are a fact of life these days and can account for up to 40-60% of web traffic on a retailer’s site. Online retailers might know how much of their web traffic is from bots, but what they probably don’t know is what those bots are doing.

When most people think about bots they typically think attacks, such as DDoS or application-layer attacks. However, these are only some of the bots that exist on a retailer’s site. In fact, bots do many different things with both positive and negative results. Bots unchecked can impact website performance, search visibility, on-site experience, and even the competitive landscape. But if a web retailer doesn’t know what types of bots are on their site, they can’t act to reduce the impact of those bots on the customer experience.

So what do bots have to do with retail?
Bots are automated web traffic on a retailer’s site. Each bot has a different purpose, some good and some bad, but all contribute to total traffic. Bots impact 1) how customers find a site; 2) what type of web experience they have while on the site; 3) long-term customer value and loyalty; and 4) how online retailers compete/are competed with.

How Customers Find a Retailer’s Product and/or Site: Once a shopper has decided they need something, their first step is often Search (i.e., Google, Bing, Yahoo!). Bots play an important role here. First, search engines create bots to crawl websites and return information on a site’s content, helping shape how those websites are prioritized in search results. Web retailers must ensure high website performance for search engine crawlers as well as users, because slow site load times can negatively affect rankings.

Second, online retailers will create bots or contract with a third-party service to crawl their own site in order to evaluate how effective their SEO efforts are. A related aspect of bot interaction involves partners who sell a retailer’s product or service through other channels. They will scrape the retailer’s site to ensure they have the most up-to-date pricing and content. The purpose is legitimate and the benefit real (extending the retailer’s reach and audience). However, online retailers need to ensure that these bots get the information they need without negatively impacting the on-site experience.

On-site Experience: Once the retailer has brought the shopper to their site, they must ensure a high-quality user experience so that the shopper can easily and quickly find the products or services they want. However, with up to 40-60% of traffic being bots, too many bots operating too freely, regardless of the type or intention, will result in a degradation of website performance, causing legitimate, human traffic to have a negative web experience.

One large auto-part company uncovered an issue with their search results because they were blocking all bots including search-engine bots, and it was affecting their website’s visibility.
On-site user experience is also driven by data - now a core competency for online retailers as they strive to deliver more personalized web experiences to their customers. Leveraging advanced marketing analytics tools, online retailers seek greater insight into who is buying their products so they can deliver a more customized user experience, leading to more higher-value sales. However, a by-product of the proliferation of bot traffic is that marketing data, which drives key tactical and strategic decisions, is corrupted. Bots skew the data and misrepresent the true nature of a web retailer’s customers, invalidating conclusions drawn from the data set.

Customer Loyalty: Loyal customers are awesome — they buy more, more often, and support the brand socially. Building trust with customers to move them into this upper echelon is challenging but very rewarding. However, third parties often use bots to get between web retailers and their customers, jeopardizing that customer relationship.

For example, many online retailers employ strategies involving flash sales or sales of limited inventory to generate buzz and draw consumers to their site, where they may purchase other goods. However, malicious bots can impact the effectiveness of these strategies by automating the purchase of products or services that are time limited (e.g., flights, event tickets, or limited-edition shoes, clothing, etc.) to resell on other sites. This leads to a poor customer experience, as legitimate buyers are unable to acquire a product/service or are made to pay more than market price.

Competition: Staying ahead of the competition in retail is challenging, particularly as consumers can so easily (and willingly) jump from brand to brand, seeking the best deals and user experiences. To differentiate, retailers offer unique online content that entices consumers to (re)visit the site regularly. Whether branded, user generated, or third party, the goal is to provide a great user experience that builds a relationship. However, competition can use bots to regularly and automatically crawl the retailer’s site to “scrape” data including product mix, pricing, content, and more - negating much of the value and uniqueness of the web content the retailer worked so hard to create, aggregate, and curate.

What does good look like?

The ideal solution would allow an online retailer to manage bot traffic to ensure the best possible outcome — maximizing the positive results and minimizing the negative — depending upon the type of bots they see.

For example, while online retailers do want to allow good bots to do their job, there are circumstances where they may need to be ratcheted back to ensure the human web traffic can shop and buy without issue. Examples of where this throttling of website access is important are key shopping times like the holiday season or if a bot is too aggressive in its crawling of the site.

When a web retailer encounters bad bots, blocking them is only a temporary solution that is ineffective in the long run — blocked bots will simply return smarter and faster. By managing how those bots are allowed to interact with the site, a web retailer can minimize the negative impact of those bots without tipping off the operator that the retailer is on to them. Two common solutions are simply slowing them down to reduce the value and timeliness of the information they are gathering or serving them alternative information - pushing them to a page with intentionally inaccurate web content.

Akamai’s Bot Manager: In direct response to the current state of bot solutions, Akamai has created a unique alternative for online retailers struggling to deal with the bot problem. The solution is designed to allow a retailer to identify, categorize, and manage the bots — both good and bad - to achieve the goals for their website. Bot Manager provides a range of management actions beyond just blocking to help organizations maximize the positive and minimize the negative impacts of their bot traffic. They are able to then analyze and report the activity to improve visibility on the bot issue. In addition to visualization and reporting on bot traffic, Bot Manager can also help organizations with their own internal marketing data. Website and page-view statistics can be significantly skewed by bot traffic, making it difficult to understand the behavior of real users interacting with the site. Bot Manager identifies bot-generated requests in order to filter out bot traffic from human traffic, which can help improve marketing's data and analysis, and lead to better business decisions.

Learn more at akamai.com/bot-manager