The Bot Problem in Ecommerce

As of 2020, only 59.2% of web traffic is generated by actual humans — the rest is made up of bots.¹

While some bots are welcomed, like search engines and crawlers, nefarious bots pose a significant threat to platform abuse, fraud loss and more.

These bots mimic the actions of legitimate users, making them notoriously hard to detect and allow their operators to perform a number of malicious activities on site/platform. Last year, these bad bots accounted for over 25% of all internet traffic and no industry was spared:¹

Click logos for articles on bot attacks.

**Bots Wreak Havoc Online by Causing:**

<table>
<thead>
<tr>
<th>TICKETING</th>
<th>LUXURY GOODS</th>
<th>ELECTRONICS</th>
<th>REVIEW FRAUD</th>
<th>USER FRAUD</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ticket bots have many avenues of attack: fake account creation, inventory squatting, transaction fraud, account takeover, cashing out, and more.</td>
<td>Luxury Brands are highly susceptible to scalping, scraping, stuffing, card cracking and other forms of merchandise fraud and data privacy. On so-called “hyped” releases, close to 100% of traffic is bots.¹</td>
<td>Electronics was once a democratized industry where consumers had fair access to products. Now, companies like Nintendo, PS5 and even computer chips/parts, have to wade off bot attacks and disruptions in site continuity.</td>
<td>While every product has a number of valid online reviews, a number of bad-intentioned bots attempt to do the same thing to disrupt global commerce. This creates customer distrust and damages brand integrity.</td>
<td>These accounts are then used to do a myriad of fraudulent activities such as generating spam, spreading malware to valid users, and much more.</td>
</tr>
</tbody>
</table>


**FRAUD LOSS**

**DATA CONTAMINATION**

**POOR USER EXPERIENCES**

**SITE CONTINUITY DISRUPTION**

**BOTWATCH: 30-DAY FREE POV**

Drop 1 line of code and in 30 days, we’ll show you the impact bots are having on your business.