You still don’t have marketing security?

Why has ‘marketing security’ become a top priority for modern-day marketers?

Five years ago, if you were to ask a marketer about their security strategy, the likely response would have been sheer confusion. *“Bots, proxies, data-center traffic? That’s for the security team to worry about.”* In 2022, however, you’d be hard-pressed to find a marketing leader who hasn’t deployed a marketing security strategy. Today, most marketers view fake, automated and malicious traffic as a strategic threat to their operation, compromising efficiency and hurting their bottom line.

27% of website traffic is fake, and it’s killing marketing efficiency

Recent data released by CHEQ across a pool of over 12,000 of its customers revealed that 27% of all website traffic is fake, consisting of botnets, data centers, automation tools, scrapers, crawlers, proxies, click farms and fraudsters. The scale of the “Fake Web” is massive, and marketers are seeing it everywhere. Just this past Super Bowl, 17 billion ad views came from bots and fake users. On Black Friday, a third of online shoppers weren’t real. Affiliate marketers are losing $1.4 billion a year to fraud. Elon Musk recently highlighted concerns over bots overrunning social media and Spotify is reportedly suffering from its own bot problem. Wherever marketers look, the Fake Web is there, and it’s affecting their campaigns, funnels, data and revenue.

Paid marketers without security ‘waste’ thousands of clicks on fake users

Perhaps one of the most visible issues for marketers, especially those running paid user acquisition, is Click Fraud. Bots, click farms and even competitors are draining their ad budgets and severely damaging campaign efficiency. Many advertisers suffer from thousands and even tens of thousands of fake clicks every month, amounting to a massive waste of spend. But it’s not just the wasted spend, it’s also budgets that could have otherwise gone to real paying customers who would have generated actual revenue. In fact, recent data shows that $42 billion is lost each year in revenue opportunities because of this issue.

But the real damage begins when those fake users infiltrate your audiences

Many paid marketers use smart campaigns or audiences to group

together users that have either previously shown interest in their products or services or share attributes with users who have. This is helpful for expanding the market they are addressing and reaching new potential buyers. At this point, it might not come as a surprise that bots and fake users can stand in the way of successfully executing this practice as well. When audiences become polluted with malicious human users or invalid bot traffic, marketers end up accidentally re-targeting and optimizing toward fake traffic. If marketing security measures are not put in place, the cycle can continue until audiences are overtaken by bots and no longer share any resemblance to a group of human users that have the ability and intention to convert. If clean audience segments are a priority, then, for many marketers, marketing security is as well.

Fake traffic is also one of the biggest drivers of poor lead quality

Every marketer can relate to the frustration of illegitimate looking inbound leads. Sometimes it’s a fake account or a bogus email address. Sometimes the information looks legitimate but when you research the lead you can’t find the company or individual. But whatever the case is, nothing causes more tension between sales and marketing than bogus leads that waste the sales team’s time and never convert. In fact, poor traffic quality is one the biggest drivers of marketing security adoption today, as teams look to eliminate illegitimate form fills and submissions and prevent them from polluting the sales pipeline.

But perhaps the biggest reason marketers are fighting bots is data quality

Beyond the monetary waste, budget inefficiency, polluted audiences and fake leads, there is one issue that stands above them all, which is perhaps the biggest driver of marketing

security adoption – and that issue is data quality. Think about it – organizations spend so much energy, time, effort, resources and money on data management and consumption – expensive BI, analytics and reporting tools, teams of analysts, CDPs and DMPs. All of this so that they can drive better tactical decisions around landing page optimization, audiences and targeting, as well as strategic decisions around budget and channel planning, growth planning and revenue forecasting. When an average of 27% of traffic-in-funnel is fake, all that data is skewed and those decisions are severely compromised. Adding a layer of visibility to detect bots and fake users and gain transparency over their funnels, is becoming an absolute integral part of the modern-day marketer's role.

More than anything, marketing security is being looked at as an opportunity

Marketers want to eliminate these threats to their operation, but above all, they want to drive better budget efficiency, better leads and higher revenue, and that's the ultimate goal of marketing security. Eliminating these inefficiencies drives a healthy, clean and transparent funnel that delivers better results. And for these reasons, asking a marketer "what's your security strategy?" in 2022, is quickly becoming an almost banal question, as Marketing Security quickly becomes an industry standard.

This article was written by Daniel Avital, chief strategy officer, and global head of marketing at CHEQ.

New on Search Engine Land

About The Author

CHEQ is the go-to-market team’s security suite, trusted by over 12,000 customers worldwide to protect their funnels, sites, and analytics from bots and fake users. Powered by award-winning cybersecurity technology, CHEQ offers the broadest suite of solutions for securing the entire funnel, from paid marketing to on-site conversion, data and analytics.
https://searchengineland.com/you-still-dont-have-marketing-security-385030