CLOUDFLARE

5 Best Practices for Preparing Your eCommerce Site for the Holidays

Develop an Action Plan for Cyber Week Success

For online retailers, the holiday season can be the jolliest of seasons—or a living nightmare. For 2019, US eCommerce sales are projected to rise by as much as 14%, totaling $166.9 billion, according to the National Retail Federation (NRF). That's three times the growth rate forecast for holiday retail overall, making online and mobile sales critical drivers for success from this Cyber Week to the 2020 holiday season and beyond.

But challenges abound. Merchants that deliver a fast, convenient, and secure customer experience will have plenty to cheer. Those that can't could fall prey to cyberattacks and watch customers defect to competitors. Here are 5 best practices for mitigating this season's biggest risks while maximizing your holiday profits.

#1 Maximize the Customer Experience, Especially on Mobile

According to a new survey from PwC, 54% of consumers plan to opt for the convenience of shopping via their smartphones, computers, and even in-home voice assistants like Alexa. Mobile accounts for 60% of all online traffic, and may account for more than half of all online sales for the first time.

As Forrester Research reports, mobile customers say visual content is key to the shopping experience. Savvy retailers will run performance tests to optimize visual content load speeds. And many will leverage content delivery networks with advanced compression and caching capabilities to ensure blazing-fast image resizing from a single master image, along with smooth, seamless video streaming.

#2 Disaster-Proof Your Cyber Week Surge

Nearly 40% of all online sales transactions are expected to be made from Thanksgiving through Cyber Week, making store uptime and availability a crucial concern for many retailers. Studies show 50% of consumers will bail on a transaction after just 10 seconds of friction. And that's if they can even access your site.

Whether you're hosting servers on-premise or in the cloud, make sure you're able to support increased workloads. In the event your site goes down, you also need to ensure traffic can fail over to an alternate site. Your hosting provider should provide you with options for co-located site migrations in the event of a disaster or outage.

#3 Deck Your Defenses Against DDoS Attacks

Effective disaster-proofing includes preparing for an onslaught of Distributed Denial-of-Service (DDoS) attacks aimed at taking your hosting servers offline. According to some estimates, 2018 saw DDoS attacks on ecommerce sites spike 70% on Black Friday and 109% on Cyber Monday.

You can invest in expanding your infrastructure to absorb peak workloads, but large-scale attacks may crash your site anyway. A better idea: Deploy a scalable, cloud-based DDoS mitigation solution to neutralize the threat from DDoS and keep your store up and welcoming to shoppers.

#4 Protect Against Bot-based Account Takeovers

Account takeovers (ATOs) are expected to rank among the top fraud threats this holiday season, as credential-stuffing bots use breached login credentials to hijack customer accounts or validate gift card numbers to go on shopping sprees. For some retailers, malicious bots can make up as much as 90% of site traffic during peak times such as Black Friday and Cyber Monday.

Additional login security measures such as CAPTCHA challenges can help mitigate this threat. But to minimize the impact on the customer experience, deploy a bot management service that uses advanced machine learning to sniff out malicious bots and block their login attempts without impacting legitimate customers.

#5 Secure Your Store, Your Customers, and Your Brand

No pre-Cyber Week checklist is complete without assessing website security, third party applications, and web services such as APIs. In addition to guarding against data breaches, other vulnerabilities to prepare for include cross site scripting (XSS) attacks in order to impersonate customers or trick them into revealing personal information. They also include SQL injections that can manipulate your product catalog or prices, and potentially complete fraudulent purchases.

Web application firewalls (WAFs) are required for PCI-DSS compliance to protect the theft of customers' payment details, and they're essential for protecting other personal information as well. What's more, all data that is exchanged or delivered through your site should be encrypted with the latest TLS 1.3 encryption standard to keep your customers safe, satisfied, and in the holiday spirit.

The Cloudflare Difference

Trusted by over 20 million Internet properties, our integrated cloud platform helps brands and retailers improve the performance of their web properties, while also safeguarding customer data and transactions during Cyber Week and every day of the year.

ENHANCE CX FOR MORE CONVERSIONS

- CDN
- Image resizing
- Video streaming
- Accelerated web content

ENSURE STORE AVAILABILITY

- Load balancing
- Managed DNS
- Virtual backbone
- Rate limiting
- Secure Your Site & Transactions
- Bot management
- Web Application Firewall
- TLS 1.3

NETWORKED INTELLIGENCE POWERED BY MACHINE LEARNING

With Cloudflare, an attack in Bangladesh bolsters your security in Omaha. An undersea cable is cut? Your customers are automatically re-routed.

Cloudflare's network analyzes traffic to over 20 million Internet properties worldwide, spanning over 1 billion unique IP addresses per day, to keep your eCommerce site up and running. .

GET STARTED IN JUST 5 MINUTES

See just how easy it is to join the Cloudflare revolution:

cloudflare.com/eCommerce/