

Tech, Turkey, and Thanks

According to Deloitte, holiday sales are projected to total **\$1.59 trillion** from November 2023 through January 2025.

Cybercrime spikes dramatically during the holiday shopping season. **Black Friday** and **Cyber Monday** are historically the biggest purchasing events of the year, and there are more ways to shop than ever. That means retailers must ensure smarter, faster, and safer experiences to win customers over.

1



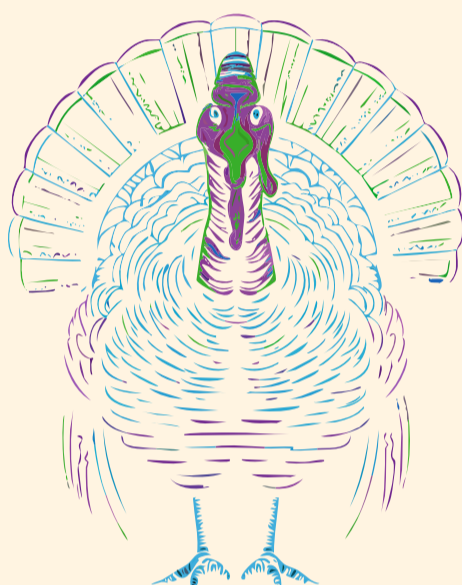
AI on the Menu: Serving Personalization

This holiday season, AI is front and center, making buyers feel a little more special through tailored experiences. In fact, 52% of consumers use AI tools instead of traditional search engines for product recommendations.

Balancing privacy and AI

New tech means new risks. Fake product suggestions. Fraudulent websites. Preventing AI model poisoning, prompt injection attacks, and hallucination is critical, and proper data inputs can help avoid breaking data privacy regulations or laws.

2



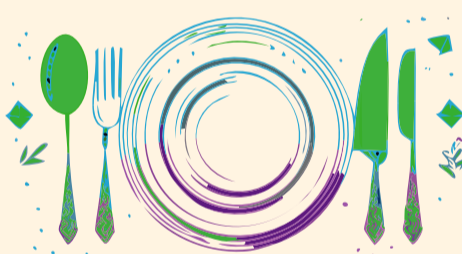
Gobbling up the Savings

With 52% of shoppers concerned about finances, savings are top of mind. Retailers can implement dynamic pricing tools that adjust prices in real time, staying competitive. However, buyer (and seller) beware. Cyber attackers create fake discount websites or schemes that promise unrealistic deals.

Browser extensions offer fraud defense

To combat fraud, many browsers use databases of known malicious sites and real-time URL analysis to warn users if they attempt to visit potentially dangerous websites.

3



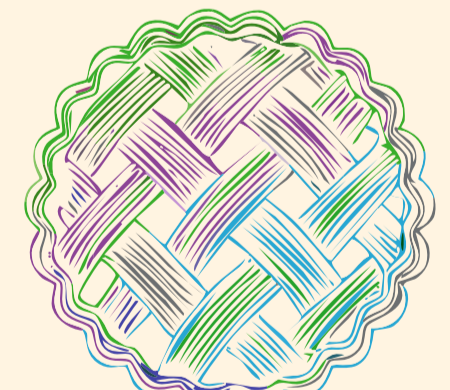
Social Commerce: Great Deals with a Side of Caution

Social media has become a go-to shopping platform, making it easy for businesses (and influencers) to sell directly to customers. The downside? Scammers.

Secure transaction integrations

To mitigate risks, both retailers and buyers can use payment systems with built-in verification processes like tokenization and biometric authentication. Consumers should also check for the authenticity of the sellers and read reviews before making purchases.

4



Pass the Pie, Not Payment Info

As holiday shopping heats up, 76% of U.S. shoppers want consistency and convenience during checkout. That often means saving payment information. According to Verizon, 57% of breaches involving stolen credit cards are from criminals stealing from e-commerce sites.

Add more security layers and encryption

Businesses can protect consumers using web application firewalls, inventorying third-party JavaScript on websites, and regularly asking vendors to audit their code. Shoppers, in turn, should be cautious with unfamiliar payment platforms.

Carve our Protection, Savor Trust

The common thread in our top four? Cyber threats. Retailers who put cybersecurity first and provide clear, transparent communication about their protective measures are bound to build customer loyalty and thrive.