Mankato Computer Technology University

Online Shopping

Introduction

Define online shopping: *"The process of purchasing goods or services via the internet."*

Highlight its global relevance: billions of users worldwide, driving economies.

History and Evolution

Origins: First online purchases in the 1990s (e.g., Amazon, eBay).

Milestones: Introduction of mobile shopping, digital wallets, and personalized algorithms.

Present-day dominance:

Benefits of Online Shopping

Convenience: 24/7 availability, shopping from home.

Variety: Global products at your fingertips.

Cost-effectiveness: Discounts, price comparisons.

Personalization: AI-driven recommendations.

Challenges of Online Shopping

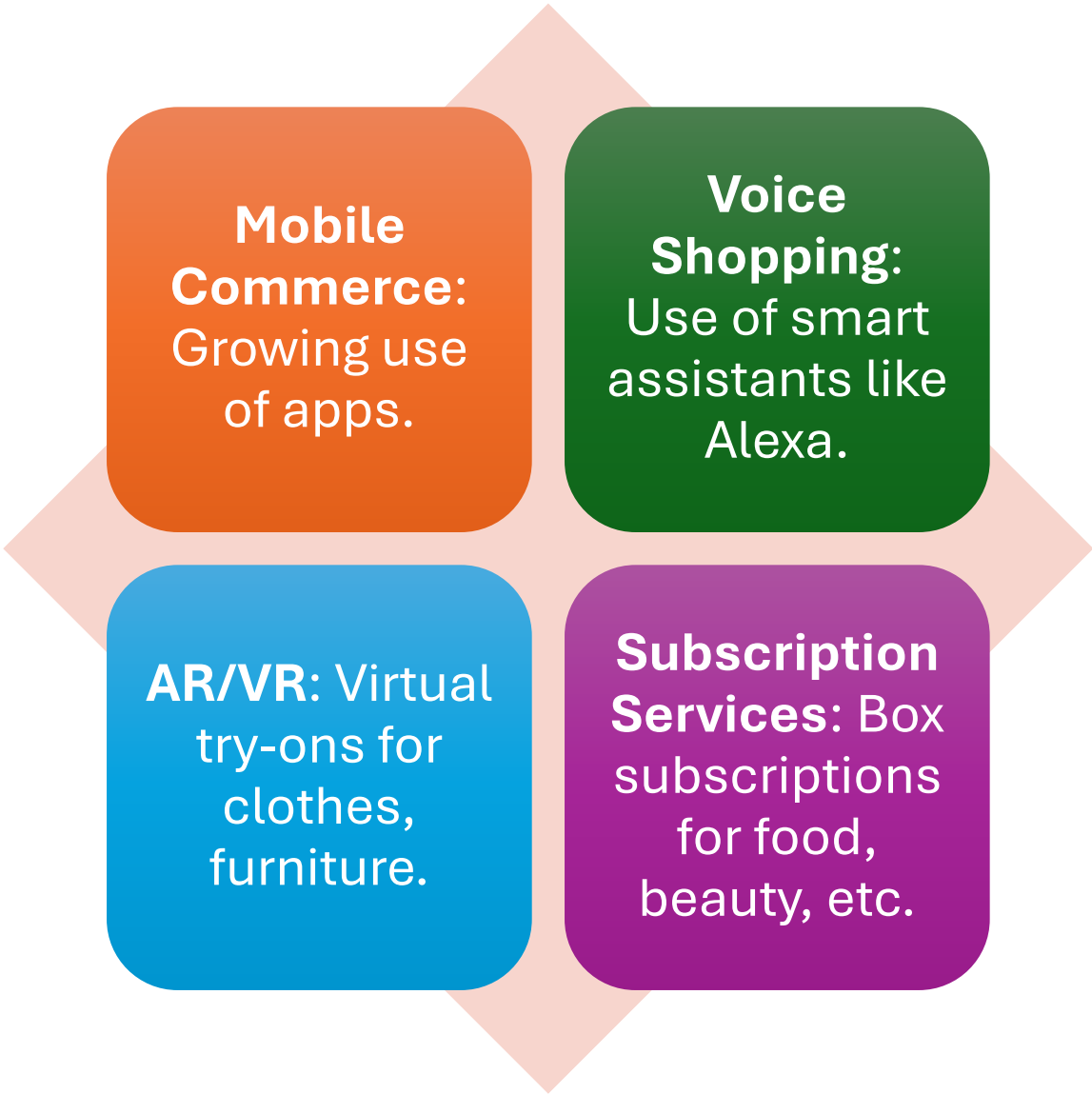
Security: Data breaches, fraud.

Delivery Issues: Delays, lost packages.

Lack of tactile experience: Cannot see, touch, or try before buying.

Environmental Concerns: Packaging waste, carbon footprint from shipping.

Trends in Online Shopping



Future of online Shopping

- Growth of AI and machine learning for hyper-personalized experiences.
- Expansion of drone and autonomous delivery.
- Cryptocurrency and blockchain for secure payments.
- Sustainability-focused shopping (eco-friendly practices).

Tips for Safe online Shopping

1

Verify website credibility (HTTPS, reviews).

2

Use secure payment methods (credit cards, trusted platforms like PayPal).

3

Be wary of deals too good to be true.

4

Regularly monitor bank statements.

Shop on Secure Websites

LOOK FOR WEBSITES WITH HTTPS IN THE URL (THE “S” STANDS FOR SECURE).

CHECK FOR A PADLOCK ICON NEAR THE URL.

STICK TO REPUTABLE AND WELL-KNOWN PLATFORMS.

Use Strong Unique Passwords

AVOID REUSING PASSWORDS ACROSS SITES.

USE A MIX OF UPPERCASE, LOWERCASE, NUMBERS, AND SYMBOLS.

CONSIDER USING A PASSWORD MANAGER FOR ADDED SECURITY.

Be Wary of Public Wi-Fi

Avoid shopping or entering sensitive information when connected to public Wi-Fi.

Use a VPN (Virtual Private Network) for secure connections.

Monitor Website Authenticity

Double-check website URLs; scammers often use slightly misspelled domains.

Avoid clicking on links from unsolicited emails or pop-up ads.

Use Secure Payment Methods

Pay with credit cards or secure payment services like PayPal; they offer fraud protection.

Avoid direct bank transfers or sending money through unverified methods.

Keep your Software updated

- Regularly update your device’s operating system, browser, and antivirus software to protect against vulnerabilities.

Research the Seller

Check reviews and ratings from previous customers.

If it’s a lesser-known store, verify its physical address and contact details.

Avoid “too good to be true” Deals

Be cautious of massive discounts or offers that seem unrealistic.

Always compare prices with other websites.

Review Privacy and Return Policies

Read the site's privacy policy to understand how your data will be used.

Check return and refund policies before making a purchase.

Monitor Bank and Credit Card Statements

Regularly check statements for unauthorized charges.

Report suspicious activity to your bank immediately.

Save Transaction Records

Keep a record of receipts, order confirmations, and communication with the seller.

These documents can help resolve disputes

Use two factor Authentication (2FA)

Enable 2FA on accounts for added security.

It requires both your password and a one-time code sent to your phone/email.

New Chrome, Safari, Firefox, Edge Warning—Do Not Shop On These Websites

- https://www.forbes.com/sites/zakdoffman/2024/11/20/new-chrome-safari-firefox-edge-warning-do-not-shop-on-these-websites/
- The team has published a list of known malicious domains:

•northfaceblackfriday[.]shop

•lidl-blackfriday-eu[.]shop

•bbw-blackfriday[.]shop

•llbeanblackfridays[.]shop

•dopeblackfriday[.]shop

•wayfareblackfriday[.]com

•makitablackfriday[.]shop

•blackfriday-shoe[.]top

•eu-blochdance[.]shop

•ikea-euonline[.]com

•gardena-eu[.]com

But beware

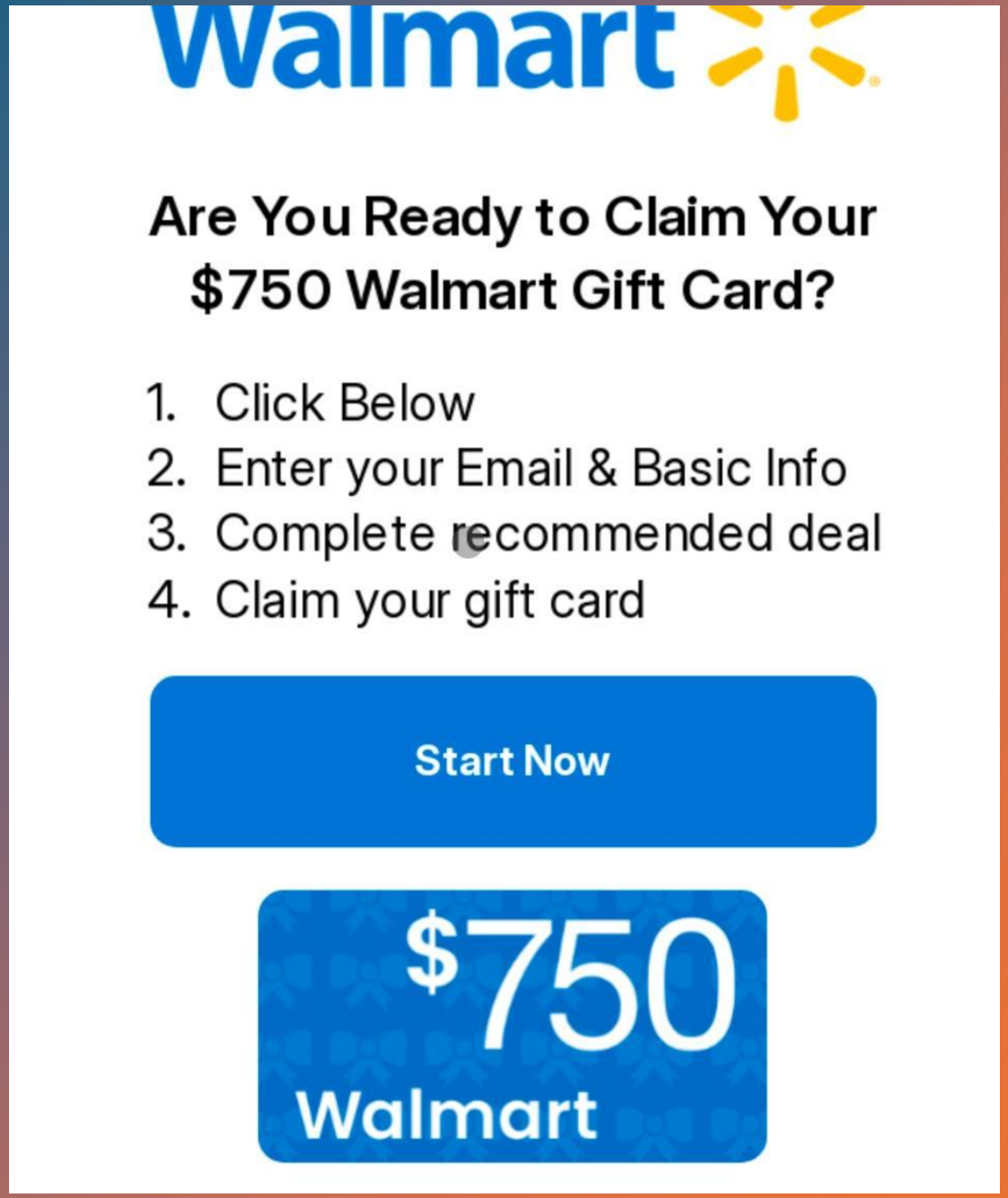
- there are upwards of 4,000 malicious domains, and so shoppers are advised to be careful when clicking on “URLs with themes like ‘discount,’ ‘Black Friday,’ or similar sales events.

Trend Micro offers these other danger signs for holiday shoppers to watch for:

- Too-Good-to-Be-True deals
- Poor design, typos, and insecure payment methods.
- Lack of or Suspicious Contact Info
- Lack of secure Payment options like credit cards.
- Unclear Return or Shipping

“cautioning shoppers that some tell-tale signs of an impersonation scam include:

- Requests for account or payment Information. We will never ask for your password or you to make a payment or bank transfer via phone, email, or on another website. You can always trust messages on our app or website – plus any emails that have the genuine Amazon smile icon to prove they’re really from us.
- False urgency. Scammers often try to create a sense of urgency to persuade you to do what they’re asking.
- A reference to a purchase (that you may or may not have made), a giveaway, or a prize.
- A notification saying, “your account is locked” and you need to click the link, make a payment, or purchase a gift card.
- Noticeable grammar or spelling errors.”



Phishing Scams are on the rise

- “these messages often create a sense of urgency, warning users of “suspicious activity”, “account suspension”, or an “unauthorized log-in attempts”. By instilling fear, scammers prompt users to click on links that lead to fake log-in pages designed to mimic Meta’s official sites.”
- “The catch is always the same: the recipient must act quickly, or they risk missing out on the ‘exclusive’ offer,” Kaspersky explains. “These tactics prey on consumers’ fear of losing out, tricking them into acting impulsively. In reality, there is no deal — just a carefully designed scam aimed at manipulating victims into making small payments to the scammers, thus losing money and giving away their payment details.”

Conclusion

Recap key points: convenience, growth, challenges, and future.

"What do you think the next big trend will be?“

Q&A