

What Is E-Commerce On The Internet?

Posted on October 11, 2019

E-commerce is the exchange of goods, services, information, and payments through electronic networks. The original article defines it broadly to include online trade, marketing, banking, insurance, information exchange, and capital flows. That broad approach remains useful because e-commerce is not limited to an online store. It includes the complete digital transaction process: discovering a product, comparing alternatives, creating an account, placing an order, signing a contract, authorizing payment, arranging delivery, obtaining customer support, and managing returns. Some transactions are entirely digital, such as purchasing software or streaming access; others combine digital ordering with the physical movement of goods. The Internet is the most visible infrastructure for e-commerce, but mobile networks, payment systems, cloud services, electronic data interchange, application-programming interfaces, and logistics platforms also make it possible. Modern e-commerce therefore connects commercial strategy, technology, law, cybersecurity, consumer protection, and supply-chain management.

What Is E-Commerce on the Internet?

Internet-based e-commerce occurs when one or more stages of a commercial transaction are conducted online. A consumer may search for a product on a marketplace, pay through a digital wallet, and receive the item from a local warehouse. A manufacturer may exchange purchase orders and invoices electronically with suppliers. A freelancer may deliver a digital service to a client in another country. A government may collect fees through an online portal. These examples differ in scale and participants, but all replace or supplement paper, cash, or face-to-face processes with electronic communication.

The legal recognition of electronic records is essential. The UNCITRAL Model Law on Electronic Commerce was designed to remove legal obstacles and support equal treatment of paper and electronic information. Its principles include non-discrimination against electronic form, functional equivalence, and technology neutrality (UNCITRAL, 1996). These principles do not mean that every electronic message automatically forms a valid contract. Parties must still satisfy applicable requirements relating to identity, consent, terms, capacity, evidence, and consumer rights. They mean that a transaction should not be rejected merely because it was conducted electronically.

Core Components of an E-Commerce System

An effective e-commerce system has several connected components. The customer-facing website or application provides product information, search, navigation, accessibility, and checkout. The product-information system maintains descriptions, prices, availability, and images. The order-management

system records purchases and routes them for fulfillment. Payment services authorize and settle transactions. Inventory and warehouse systems determine whether goods are available and where they should be shipped. Customer-service tools manage questions, complaints, and returns. Analytics help the business understand performance, but their use must respect privacy and consent.

A weakness in any component can damage the whole experience. A beautiful website cannot compensate for inaccurate inventory, insecure payment handling, hidden delivery charges, or an impossible return process. Businesses should therefore treat e-commerce as an operating model rather than merely a marketing channel. Technology, fulfillment, finance, legal compliance, and customer support must share accurate data and clear responsibilities.

Business-to-Consumer E-Commerce

Business-to-consumer, or B2C, e-commerce occurs when a company sells directly to individual customers. This includes retailers, subscription services, online education, travel booking, entertainment, food delivery, and many other activities. B2C systems emphasize usability, trust, transparent pricing, secure payment, delivery information, and customer service. Consumers often compare several sellers within minutes, so misleading descriptions or unexplained charges can quickly damage reputation.

The original article correctly identifies convenience and broad choice as advantages. Consumers can shop outside normal business hours, compare specifications, read policies, and purchase from distant sellers. However, reviews and ratings require critical evaluation because they may be manipulated, incentivized, or unrelated to the buyer's needs. Responsible platforms verify transactions where possible, disclose sponsored content, and provide procedures for challenging fraudulent reviews.

Business-to-Business E-Commerce

Business-to-business, or B2B, e-commerce covers transactions between organizations. A manufacturer may order raw materials through a supplier portal; a retailer may exchange inventory data with a distributor; a company may subscribe to cloud software. B2B transactions often involve negotiated prices, credit terms, recurring orders, technical specifications, approval workflows, and integration with accounting or procurement systems. The value of individual transactions may be high, while the number of customers is lower than in consumer retail.

B2B e-commerce can reduce paperwork, errors, and procurement time. Electronic catalogs and standardized data make it easier to compare approved products and track spending. Yet integration creates dependency. Incorrect product codes or automated orders can produce large mistakes quickly. Access controls, approval limits, audit trails, supplier verification, and contingency procedures are therefore essential.

Consumer-to-Consumer and Platform Commerce

Consumer-to-consumer, or C2C, e-commerce allows individuals to sell or exchange goods and services with one another through a platform. Online auctions, resale marketplaces, classified services, and peer-to-peer rental systems are examples. The platform may provide identity checks, search, messaging, payment protection, ratings, and dispute resolution. It earns revenue through fees, advertising, or payment services.

C2C commerce expands the useful life of products and gives individuals access to large markets, but it creates trust problems because sellers may be unknown and goods may be used, counterfeit, stolen, or inaccurately described. Platforms should publish clear rules, protect payment information, respond to illegal listings, and provide fair dispute mechanisms. Buyers should use protected payment channels rather than transferring funds outside the platform without safeguards.

Other E-Commerce Relationships

Additional models include consumer-to-business, in which individuals offer services or content to companies; business-to-government, involving electronic procurement and contracting; and direct-to-consumer commerce, in which producers sell without traditional retail intermediaries. Social commerce integrates shopping with social-media content and messaging. Mobile commerce refers to transactions completed through smartphones or tablets. These categories overlap, but they help identify who creates value, who controls the platform, who bears risk, and what protections are needed.

Advantages for Consumers

The original article emphasizes geographic reach, speed, and the ability to find lower-cost goods. Online shopping can be especially valuable for people who live far from stores, have mobility limitations, work irregular hours, or require specialized products. Search and comparison tools can reduce the time required to investigate alternatives. Digital records provide order confirmations, receipts, and tracking information that are easier to retain than paper documents.

Convenience should not be confused with informed choice. Personalized interfaces may rank products according to commercial priorities rather than objective quality. Limited-time messages and complicated cancellation processes can pressure consumers. Ethical design should present total price, recurring charges, delivery time, cancellation rights, and material limitations before purchase. Accessibility is also essential: websites should work with keyboards, screen readers, captions, zoom, and clear language.

Advantages for Businesses

E-commerce allows a business to reach customers beyond the immediate location and operate continuously. Digital systems can automate order confirmation, inventory updates, invoicing, and customer communication. Small businesses can test products without building a large physical retail network. Data from sales and service interactions can help forecast demand and identify problems. Electronic delivery makes some products scalable at relatively low marginal cost.

Nevertheless, opening an online store is not automatically inexpensive. Businesses may need to pay for development, hosting, payment processing, cybersecurity, advertising, marketplace commissions, storage, packaging, returns, fraud prevention, tax compliance, and customer support. Competition is global, and acquiring attention can be costly. A realistic business case should calculate the full cost of fulfillment and retention rather than focusing only on website creation.

Limitations and Risks for Consumers

Consumers cannot always inspect a product physically before buying. Images may conceal size, texture, quality, or defects. Delivery can be delayed, damaged, or sent to the wrong address. Fraudulent stores may collect payment without sending goods. Counterfeit products can create safety risks. Personal data may be misused or exposed in a breach. Subscription services may be easy to start and difficult to cancel.

These risks can be reduced by checking seller identity, using protected payment methods, reading return and privacy policies, avoiding suspicious links, and keeping transaction records. However, responsibility cannot be placed entirely on consumers. Platforms, payment providers, regulators, and sellers must design systems that prevent deception and provide remedies when problems occur.

Limitations and Risks for Businesses

Businesses face payment fraud, account takeover, chargebacks, denial-of-service attacks, data theft, fake reviews, and supply-chain disruption. A seller may receive an apparently valid order that later proves unauthorized. A software vulnerability can expose customer data and interrupt operations. Dependence on one marketplace or advertising platform can become dangerous if fees, ranking rules, or account status change suddenly.

Operational risk is equally important. Fast online demand can overwhelm inventory and customer service. Inaccurate stock information leads to cancellations and loss of trust. High return rates increase transport, labor, and waste. Businesses should develop incident-response plans, secure backups, vendor controls, fraud monitoring, inventory accuracy, and alternative communication channels.

E-Commerce and Perishable Goods

The original article suggests that e-commerce is unsuitable for food and other quickly spoiled goods. That conclusion is now too absolute. Grocery delivery, restaurant ordering, meal kits, and temperature-controlled shipping demonstrate that perishable products can be sold online. The real issue is whether the seller can maintain food safety, cold-chain integrity, delivery speed, traceability, and accurate substitution. These requirements can make the model expensive or impractical in some locations, but the category itself is not excluded from e-commerce.

Customers buying perishables need clear delivery windows and instructions for reporting unsafe temperatures or damaged packaging. Sellers must comply with relevant food-handling and labeling rules. Technology supports ordering, but it cannot replace physical controls during storage and transport.

Electronic Payment Methods

The original article lists cash on delivery, bank transfers, cards, smart cards, and electronic money. These methods remain relevant, while digital wallets, real-time bank payments, and mobile money have become more common. Cash on delivery can build trust in markets where card use is limited, but it creates collection and failed-delivery costs. Bank transfers may suit high-value B2B transactions but can offer less consumer recourse when sent to a fraudulent seller. Cards provide broad acceptance and dispute procedures, while exposing merchants to processing fees and chargebacks. Digital wallets can reduce the need to share card details with every seller and may support biometric or multi-factor authentication.

Payment design should reflect transaction value, customer access, fraud risk, settlement time, currency, and legal requirements. Businesses should avoid storing sensitive payment data unnecessarily. Using a reputable payment service can reduce direct exposure, although the seller remains responsible for securing accounts, integrations, and administrative access.

Cybersecurity and Privacy

Trust is essential to electronic commerce. Security begins with basic controls: supported software, encrypted connections, secure coding, multi-factor authentication for administrators, restricted privileges, backups, monitoring, and response planning. Employees should be trained to recognize phishing and payment-change fraud. Vendors and plug-ins require assessment because a compromise outside the business can affect customer transactions.

Privacy requires purpose limitation and transparency. Businesses should collect only the data needed for service, security, legal obligations, and clearly explained uses. Behavioral tracking and

personalized advertising can create value but also concern, especially when several companies exchange data. A privacy notice should describe actual practice rather than provide vague permission for unlimited reuse. Customers should have reasonable control over optional marketing and account information.

Logistics, Returns, and Sustainability

Physical e-commerce depends on warehouses, carriers, packaging, and last-mile delivery. Fast delivery can increase cost and environmental impact when orders are split or vehicles travel inefficient routes. Returns add further transport and may result in usable products being discarded. Businesses can improve sustainability by providing accurate product information, encouraging consolidated delivery, using appropriate packaging, repairing or reselling returned goods, and measuring emissions rather than relying on unsupported environmental claims.

A fair return policy balances customer confidence with protection against abuse. The terms should be visible before purchase and explain time limits, condition requirements, refund timing, and who pays shipping. Customer-service systems should connect returns with inventory and accounting so that records remain accurate.

The Future of E-Commerce

E-commerce continues to develop through automated contracting, artificial intelligence, augmented product visualization, digital identity, and cross-border data exchange. UNCITRAL's Model Law on Automated Contracting addresses legal obstacles arising when automated systems participate in forming and performing contracts (UNCITRAL, 2024). These technologies can improve convenience, but they also raise questions about errors, explanation, responsibility, and human review. A chatbot should not make it impossible for a customer to reach a person when the system cannot resolve a dispute.

The future is likely to combine physical and digital channels rather than eliminate stores. Customers may research online and collect in person, inspect in a store and order later, or use one account across several channels. Successful organizations will integrate information and service while giving customers clear choices.

Conclusion

E-commerce on the Internet is a system for conducting and supporting commercial transactions electronically. It includes B2C, B2B, C2C, mobile, platform, and government-related activity, along with digital payment, marketing, contracting, and service. Its advantages include reach, convenience, automation, comparison, and new opportunities for small businesses. Its disadvantages include fraud,

privacy loss, cybersecurity threats, unequal digital access, logistics failures, platform dependency, and difficulty evaluating products remotely. The original article was right that e-commerce has become part of ordinary life, but its success depends on more than speed. Reliable electronic commerce requires lawful contracts, accessible design, secure payment, accurate information, accountable platforms, and effective remedies when digital transactions fail.

References

Laudon, K. C., & Traver, C. G. (2023). *E-commerce 2023-2024: Business, technology, society*. Pearson.

United Nations Commission on International Trade Law. (1996). *UNCITRAL Model Law on Electronic Commerce with Guide to Enactment*.

United Nations Commission on International Trade Law. (2017). *UNCITRAL Model Law on Electronic Transferable Records*.

United Nations Commission on International Trade Law. (2024). *UNCITRAL Model Law on Automated Contracting*.