

Electronic Commerce

Lecture 5

IT392

E-commerce Security and Payment Systems

Prepared by
Dr. Eng. Youssef Ntefeh

Chapter 5

- In our digitized world, the use of e-commerce platforms has increased considerably.
- However, this convenience comes with its own sets of challenges, specifically related to security.
- In the first part of this lecture, we will be diving into the e-commerce security environment, exploring what exactly good e-commerce security involves and the threats that exist within this environment.
- We will discuss various threats ranging from malicious code, hacking, and various security issues related to social networks, mobile platforms.
- To combat these threats, we will further delve into technology solutions that ensure secure internet communications, networks, servers, and clients.

Chapter 5

- Finally, in terms of payment systems in e-commerce, we will analyze how online credit card transactions work along with other alternative online payment systems and also touch upon the fast-evolving domain of blockchain and cryptocurrencies.
- The ultimate goal is to help you understand how to protect your e-commerce platform from various potential threats and achieve a safe transaction environment.

Learning Objectives

- Understand the scope of e-commerce crime and security problems, the key dimensions of e-commerce security, and the tension between security and other values.
- Identify the key security threats in the e-commerce environment.
- Describe how technology helps to secure Internet communications channels and protect networks, servers, and clients.
- Identify the major e-commerce payment systems in use today.

Chapter 5: E-COMMERCE SECURITY AND PAYMENT SYSTEMS

The E-commerce Security Environment

The Scope of the Problem
What is Good E-commerce Security?
Dimensions of E-commerce Security
The Tension Between Security and Other Values

Security Threats in the E-commerce Environment

Malicious Code
Phishing – Hacking - Data Breaches
Credit Card Fraud - Identity Fraud
Spoofing – Pharming – Spam
Sniffing and Man-in-the-Middle Attacks
Denial of Service Attacks - Insider Attacks
Social Network Security - Mobile Platform Security

Technology Solutions

Encryption
Virtual Private Network

E-commerce Payment Systems

Online Credit Card Transactions
Alternative Online Payment Systems
Smartphone Wallet
Blockchain and Cryptocurrencies

The E-commerce Security Environment

The Scope of the Problem

- The Internet's ease of access presents an opportunity for both lawful global interactions and criminal activities
- Over 4.5 billion Internet users in 2022 are potential targets for cybercriminals who can steal money, products, and information almost risklessly and anonymously
- Cybercrime results in costs beyond the immediate financial loss, including the additional expenses for securing networks, loss of business-relevant sensitive information, reputational damage, and disruptions in service.

The E-commerce Security Environment

The Scope of the Problem

- Accurately estimating the extent of cybercrime is challenging due to underreporting from companies due to the fear of losing the trust of their customers and because even if the crime is reported, it may be difficult to quantify the actual dollar amount of the loss.
- Criminals who steal information on the Internet do not always use this information themselves but, instead, derive value by selling the information to others on the so-called underground or shadow economy market,

The E-commerce Security Environment

The Scope of the Problem

- Data is currency to cybercriminals and has a “street value” that can be monetized.
- Prices for various types of stolen data typically vary depending on the quantity being purchased and its “freshness.”
- For example, the average price for an individual U.S. credit card number with a cardholder name, expiration date, zip code is around \$17.
- Bank account or online account (such as PayPal) login credentials go for around 10% of the account’s balance.

The E-commerce Security Environment

The Scope of the Problem

- Experts believe that the cost of stolen information has generally fallen as the tools of harvesting have increased the supply
- Cybercrime is dynamic and changing all the time, with new risks appearing almost daily.
- The cost of losses to businesses is significant and growing.
- The managers of e-commerce companies must prepare for an ever-changing variety of criminal assaults and keep current in the latest security techniques.

The E-commerce Security Environment

What is Good E-commerce Security?

- E-commerce security involves mitigating risks associated with digital transactions including theft, fraud, embezzlement, trespass, and vandalism.
- To achieve highest degree of security, use:
 - New technologies
 - Organizational policies and procedures: to ensure the technologies are not subverted.
 - Industry standards and government laws: are required to enforce payment mechanisms, as well as to investigate and prosecute violators of laws

Good e-commerce security requires a set of laws, procedures, policies, and technologies that, to the extent feasible, protect individuals and organizations from unexpected behavior in the e-commerce marketplace.
- Other factors
 - Time value of money: Sometimes it is sufficient to protect a message for a few hours or days.
 - Cost of security versus potential loss
 - Security often breaks at weakest link: Our locks are often much stronger than our management of the keys.

The E-commerce Security Environment

Six key dimensions to e-commerce security:

- **1. Integrity:** refers to the ability to ensure that the information being displayed on a website, or transmitted or received over the Internet, has not been altered in any way by an unauthorized party.

For example, if an unauthorized person intercepts and changes the contents of an online communication, such as by redirecting a bank wire transfer into a different account, the integrity of the message has been compromised because the communication no longer represents what the original sender intended.

The E-commerce Security Environment

Six key dimensions to e-commerce security:

- **2. Nonrepudiation(itiraz etmeme):** the ability to ensure that e-commerce participants do not deny (i.e., repudiate) their online actions.
- For instance, the availability of free e-mail accounts with alias names makes it easy for a person to post comments or send a message and perhaps later deny doing so.
- Even when a customer uses a real name and e-mail address, it is easy for that customer to order merchandise online and then later deny doing so.

The E-commerce Security Environment

Six key dimensions to e-commerce security:

- **3. Authenticity:** refers to the ability to identify the identity of a person or entity with whom you are dealing on the Internet. How does the customer know that the website operator is who it claims to be? How can the merchant be assured that customers really are who they say they are? Someone who claims to be someone he is not is “spoofing” or misrepresenting himself.
- **4. Confidentiality:** refers to the ability to ensure that messages and data are available only to those who are authorized to view them. Confidentiality is sometimes confused with privacy, which refers to the ability to control the use of information a customer provides about himself or herself to an e-commerce merchant.

The E-commerce Security Environment

Six key dimensions to e-commerce security:

- **5. privacy** : The ability to control the use of information about oneself
- **6. Availability**: the ability to ensure that an e-commerce site or app continues to function as intended

The E-commerce Security Environment

The Tension Between Security and Other Values

- Security is not an unmitigated good. security adds overhead and expense to business operations and often complicates the process of making a purchase.
- The more security measures added, the more difficult a site is to use, and the slower it becomes
- Too much security can harm profitability; not enough can put a business out of business
- Possible solution: adaptive approach to security:
 - Segment users by risk profile
 - Adjust security settings to users' preferences

Chapter 5: E-COMMERCE SECURITY AND PAYMENT SYSTEMS

The E-commerce Security Environment

The Scope of the Problem
What is Good E-commerce Security?
Dimensions of E-commerce Security
The Tension Between Security and Other Values

Security Threats in the E-commerce Environment

Malicious Code
Phishing – Hacking - Data Breaches
Credit Card Fraud - Identity Fraud
Spoofing – Pharming – Spam
Sniffing and Man-in-the-Middle Attacks
Denial of Service Attacks - Insider Attacks
Social Network Security - Mobile Platform Security

Technology Solutions

Encryption
Virtual Private Network

E-commerce Payment Systems

Online Credit Card Transactions
Alternative Online Payment Systems
Smartphone Wallet
Blockchain and Cryptocurrencies

What Is Malvertising_ The Hidden Dangers of Online Ads



Online advertisements have become more targeted and invasive

Security Threats in the E-commerce Environment

- **Malvertising:** online advertising that contains malicious code
- A **virus** is a computer program that can replicate or make copies of itself and spread to other files. In addition to the ability to replicate, most computer viruses deliver a “payload.”
- The payload may be relatively benign, such as the display of a message or image, or it may be highly destructive—destroying files, reformatting the computer’s hard drive, or causing programs to run improperly.
- **Worm** is designed to spread from computer to computer. A worm does not necessarily need to be activated by a user or program in order to replicate itself.

DIFFERENCE BETWEEN

Viruses

Malware

Trojans

Ransomware

Spyware

& Worms!

Security Threats in the E-commerce Environment

- **Ransomware** is a type of malware that blocks or limits access to a computer or network by encrypting files and then demanding a ransom payment, typically in a cryptocurrency such as Bitcoin, in exchange for the decryption key.
- **Backdoor** is a malware feature that allows an attacker to covertly access a compromised computer or network.
- **Bots** are a type of malicious code that can be covertly installed on your computer when attached to the Internet.
- Once installed, the bot responds to external commands sent by the attacker. Your computer becomes a “zombie” and is able to be controlled by an external third party
- **Botnets** are collections of captured computers used for malicious activities such as sending spam, participating in a DDoS attack , stealing information from computers, and storing network traffic for later analysis.



Security Threats in the E-commerce Environment

- **Social engineering** relies on human curiosity, greed, gullibility, and fear in order to trick people into taking an action that enables a hacker to gain access to a computer system
- **Phishing** is any deceptive, online attempt by a third party to obtain confidential information for financial gain.
- Phishing attacks usually do not involve malicious code but instead typically rely on social engineering techniques.

What is Social Engineering

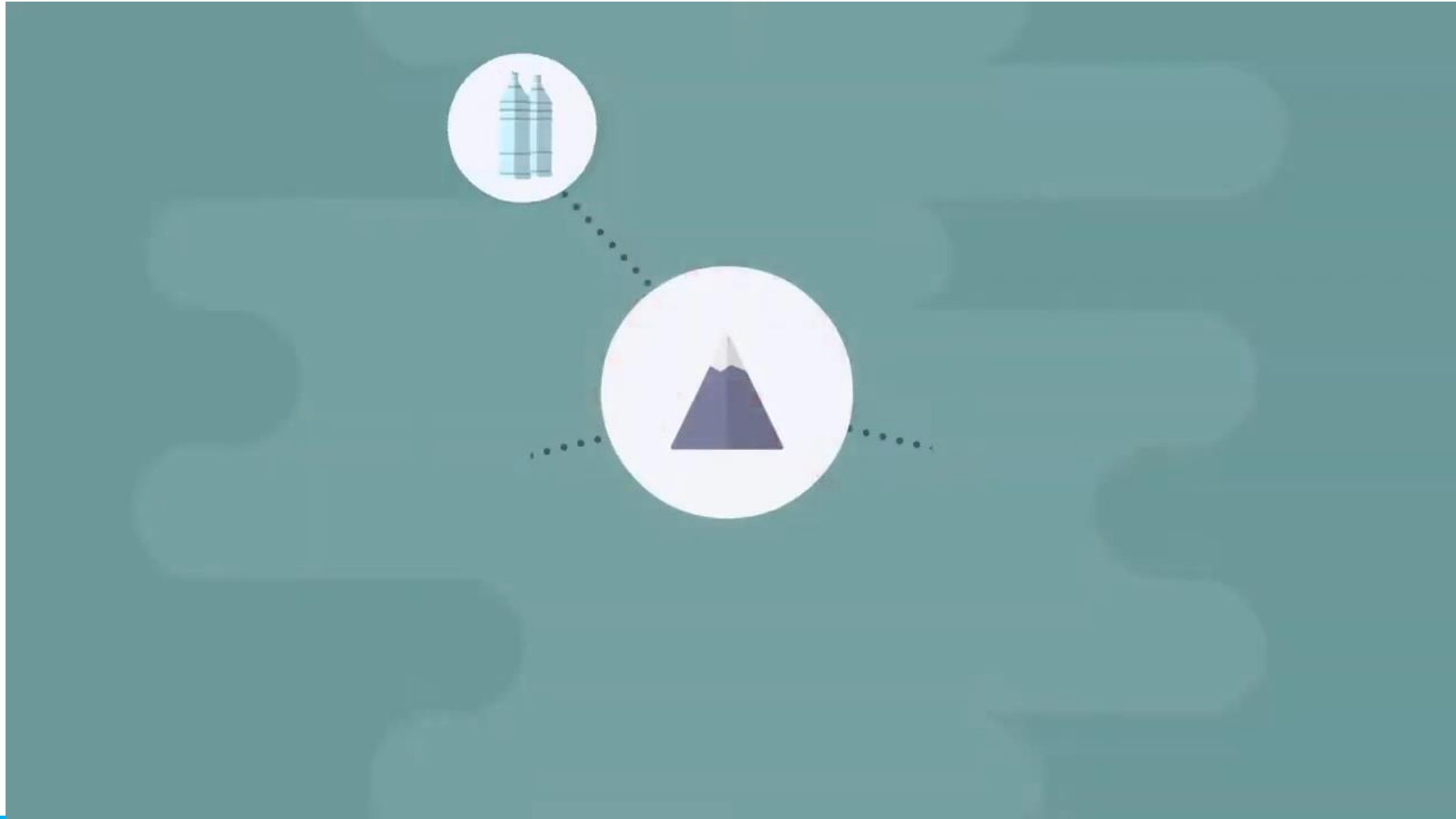
Security Threats in the E-commerce Environment

- **Hacker** is an individual who intends to gain unauthorized access to a computer system.
- **Cracker** is a hacker with criminal intent
- **Cybervandalism:** intentions to disrupt, deface, or destroy sites.
- **Hacktivism** adds a political twist to hacking.
- **Hacktivists** typically attack governments, organizations, and even individuals for political purposes
- **Data breach** occurs whenever organizations lose control over corporate information, including the personal information of customers and employees, to outsiders.

Security Threats in the E-commerce Environment

- Fear that credit card information will be stolen prevents users from making online purchases in many cases.
- Online merchants use a variety of techniques to combat credit card fraud, including using automated fraud detection tools, manually reviewing orders, rejecting suspect orders, and requiring additional levels of security such as e-mail address, zip code, and CVV security codes.
- In the past, the most common cause of credit card fraud was a lost or stolen card. Today it is the systematic hacking and looting of a corporate server where the information on millions of credit card purchases is stored.

Online Credit Card Fraud



Security Threats in the E-commerce Environment

- **Identity fraud** involves the unauthorized use of another person's personal data, such as social security, driver's license, and/or credit card numbers, as well as usernames and passwords, for illegal financial benefit.
- **Spoofing** involves attempting to hide a true identity by using someone else's e-mail or IP address.
- IP spoofing involves the creation of TCP/IP packets that use someone else's source IP address to give the impression that the packets are coming from a trusted host.
- **Pharming**, automatically redirecting a web link to an address different from the intended one, with the site masquerading as the intended destination.
- **Spam (junk) websites** offer some product or service but, in fact, are just a collection of advertisements for other sites, some of which contain malicious code.

Security Threats in the E-commerce Environment

- A **sniffer** is a type of eavesdropping program that monitors the information traveling over a network.
- A **man-in-the-middle (MitM) attack** also involves eavesdropping but is more active than a sniffing attack.
- The attacker can intercept communications between two parties who believe they are directly communicating with one another, when in fact the attacker is controlling the communications.
- In a **Denial of Service (DoS) attack**, hackers flood a website with useless pings or page requests that inundate and overwhelm the site's web servers
- A **Distributed Denial of Service (DDoS) attack** uses hundreds or even thousands of computers to attack the target network from numerous launch points.

Security Threats in the E-commerce Environment

INSIDER ATTACKS

- the largest financial threats to business institutions come not from robberies but from embezzlement by insiders.
- Bank employees steal far more money than do bank robbers.
- The same is true for e-commerce companies. Some of the largest disruptions to service, destruction to sites, and diversions of customer financial data and personal information have come from insiders—once-trusted employees.

Security Threats in the E-commerce Environment

SOCIAL NETWORK SECURITY ISSUES

- Social networks like Facebook, Instagram, Twitter, TikTok, LinkedIn, and Pinterest provide a rich and rewarding environment for hackers. Viruses, site takeovers, identity fraud, malware-loaded apps, click hijacking, phishing, and spam are all found on social networks.
- Other techniques include fake Reactions buttons that, when clicked, install malware.
- By sneaking in among our friends, hackers can masquerade as friends and dupe users into scams.
- Social networks are open: Anyone, even criminals, can set up an account.

Security Threats in the E-commerce Environment

MOBILE PLATFORM SECURITY ISSUES

- Mobile users are filling their devices with personal and financial information and using them to conduct an increasing number of transactions, from retail purchases to mobile banking, making them excellent targets for hackers.
- The majority of mobile malware still targets Android devices, which are much more likely to be infected with malware compared to iOS devices.
- This is due in part to the fact that Android users can download apps from third-party stores that are poorly regulated, whereas Apple users are confined to the more tightly controlled App Store.
- Google re-architected the Android operating system to separate hardware-specific code from the rest of Android, allowing Google to patch vulnerabilities and other security issues more quickly.

Chapter 5: E-COMMERCE SECURITY AND PAYMENT SYSTEMS

The E-commerce Security Environment

Security Threats in the E-commerce Environment

Technology Solutions

E-commerce Payment Systems

The Scope of the Problem

What is Good E-commerce Security?

Dimensions of E-commerce Security

The Tension Between Security and Other Values

Malicious Code

Phishing – Hacking - Data Breaches

Credit Card Fraud - Identity Fraud

Spoofing – Pharming – Spam

Sniffing and Man-in-the-Middle Attacks

Denial of Service Attacks - Insider Attacks

Social Network Security - Mobile Platform Security

Encryption

Virtual Private Network

Online Credit Card Transactions

Alternative Online Payment Systems

Smartphone Wallet

Blockchain and Cryptocurrencies

Technology Solutions

- **Encryption** is transforming plain text or data into **ciphertext** that cannot be read by anyone other than the sender and the receiver.
- Encryption can provide four of the six key dimensions of e-commerce security (*Integrity. - Nonrepudiation— Authentication— Confidentiality*)
- **substitution cipher**, every occurrence of a given letter is replaced systematically by another letter.
- **Transposition cipher**, the ordering of the letters in each word is changed in some systematic way.
- **symmetric key cryptography**: both the sender and the receiver use the same key to encrypt and decrypt the message.
- **DES** uses a 56-bit encryption key. improved by the *Triple DES Encryption Algorithm (TDEA)* essentially encrypting the message three times, each with a separate key.

Encryption



Technology Solutions

- **Advanced Encryption Standard (AES):** offers key sizes of 128, 192, and 256 bits.
- **Public key cryptography** (also referred to as *asymmetric cryptography*) : two mathematically related digital keys are used: a public and a private key. The keys are used to encrypt a message, cannot be used to decrypt the message
- A **hash function** is an algorithm that produces a fixed-length number called a *hash or message digest*.

Technology Solutions



Technology Solutions

Public key cryptography with digital signatures

- 1. The sender creates an original message.
- 2. The sender applies a hash function, producing a 128-bit hash result.
- 3. The sender encrypts the message and hash result using the recipient's public key.
- 4. The sender encrypts the result, again using the sender's private key.
- 5. The result of this double encryption is sent over the Internet
- 6. The receiver uses the sender's public key to authenticate the message.
- 7. The receiver uses the receiver's private key to decrypt the hash function and the original message. The receiver checks to ensure that the original message and the hash function results conform to one another.

VPN



Chapter 5: E-COMMERCE SECURITY AND PAYMENT SYSTEMS

The E-commerce Security Environment

Security Threats in the E-commerce Environment

Technology Solutions

E-commerce Payment Systems

The Scope of the Problem

What is Good E-commerce Security?

Dimensions of E-commerce Security

The Tension Between Security and Other Values

Malicious Code

Phishing – Hacking - Data Breaches

Credit Card Fraud - Identity Fraud

Spoofing – Pharming – Spam

Sniffing and Man-in-the-Middle Attacks

Denial of Service Attacks - Insider Attacks

Social Network Security - Mobile Platform Security

Encryption

Virtual Private Network

Online Credit Card Transactions

Alternative Online Payment Systems

Smartphone Wallet

Blockchain and Cryptocurrencies

E-commerce Payment Systems

MAJOR TRENDS IN E-COMMERCE PAYMENTS

- Payment by credit and/or debit card remains the dominant form of online payment.
- Online payment volume surges because of the Covid-19 pandemic.
- Mobile retail adoption and payment volume skyrockets.
- PayPal remains the most popular alternative payment method online.
- Apple, Google, and Samsung extend their reach in mobile payment apps.
- Buy Now Pay Later (BNPL) payment services increase in popularity.
- Interest in cryptocurrencies such as Bitcoin surges, even as prices crash and concerns about security increase.

E-commerce Payment Systems

ONLINE CREDIT CARD TRANSACTIONS

- Online credit card transactions are processed in much the same way that in-store credit card purchases are, with the major differences being that online merchants never see the actual card being used and no signature is available.
- These types of purchases are called Cardholder Not Present (CNP) transactions and are the major reason that charges can be disputed later by consumers.
- Because the merchant never sees the credit card or receives a signed agreement from the customer to pay, when disputes arise, the merchant faces the risk that the transaction may be disallowed and reversed even though the merchant has already shipped the goods or the customer has already downloaded the digital product.
- A **merchant account** is simply a bank account that allows companies to process credit card payments and receive funds from those transactions.

E-commerce Payment Systems

- **Limitations of Online Credit Card Payment Systems**
- The most important limitations involve security, merchant risk, administrative and transaction costs, and social equity.
- The existing system offers poor security. Neither the merchant nor the consumer can be fully authenticated.
- The merchant could be a criminal organization designed to collect credit card numbers, and the consumer could be a thief using stolen or fraudulent cards.

E-commerce Payment Systems

- **Limitations of Online Credit Card Payment Systems**

- The risk facing merchants is high. Consumers can repudiate charges even though the goods have been shipped or the product downloaded.
- Credit card companies have introduced EMV cards (cards with a computer chip) to reduce credit card fraud.
- The chip stores account data and generates a unique transaction code for each use.
- But criminals have intensified their focus on card-not-present (CNP) fraud, which comprises an ever-increasing share of the losses due to credit card fraud

E-commerce Payment Systems

Alternative Online Payment Systems

- The limitations of the online credit card system have opened the way for the development of a number of alternative online payment systems.
- PayPal enables individuals and businesses with e-mail accounts to make and receive payments up to a specified limit.
- PayPal is an example of an **online stored value payment system**, which permits consumers to make online payments to merchants and other individuals using their bank account or credit/debit cards.

E-commerce Payment Systems

Alternative Online Payment Systems

- It is available in more than 200 countries around the world.
- You establish a PayPal account by specifying a credit, debit, or checking account that you wish to have charged or paid when conducting online transactions.
- When you make a payment using PayPal, you e-mail the payment to the merchant's PayPal account.

E-commerce Payment Systems

Alternative Online Payment Systems

- PayPal then transfers the amount from your credit or checking account to the merchant's bank account.
- The beauty of PayPal is that no personal credit information has to be shared among the users and that the service can be used by individuals to pay one another even in small amounts.
- However, one problem with PayPal is its relatively high cost.
- For example, when using a credit card as the source of funds to send or request money, the cost ranges from 1.9% to 3.49% of the amount (depending on the type of transaction), plus a small, fixed fee (typically \$0.49) per transaction.

Credit Card vs Mobile Payment (Digital Wallet) Which is Safer

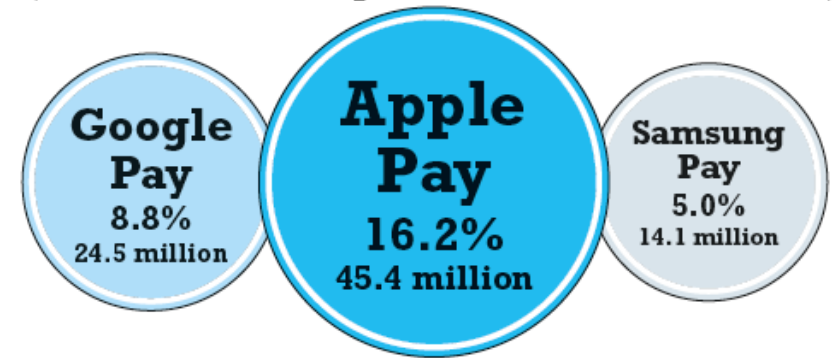


E-commerce Payment Systems

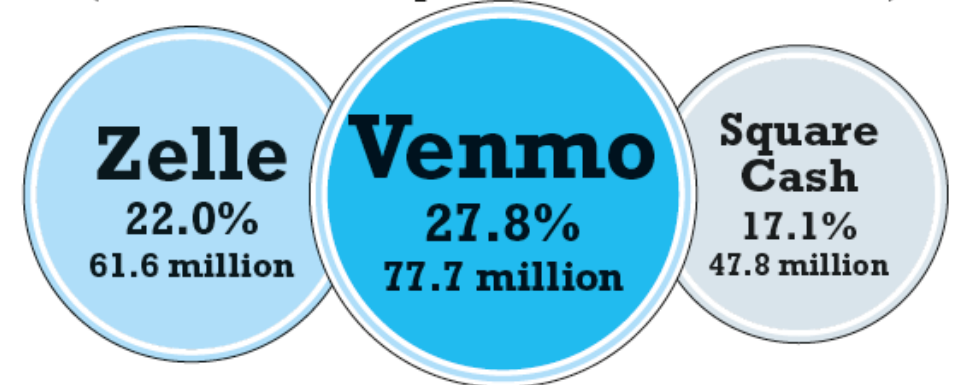
Mobile Payment Systems: Your Smartphone Wallet

- **Universal proximity mobile wallets:** such as Apple Pay, Google Pay, and Samsung Pay, which can be used at a variety of merchants
- **Branded store proximity mobile wallets** are mobile apps that can be used only at a single merchant. For instance, Walmart, Target, Starbucks, and Dunkin' all have very successful mobile wallet apps
- **P2P mobile payment apps**, such as Venmo, Zelle, and Square Cash, are used for payments among individuals who have the same app

Universal Proximity Mobile Payment Apps
(Percent of U.S. Population/Number of Users)



P2P Mobile Payment Apps
(Percent of U.S. Population/Number of Users)



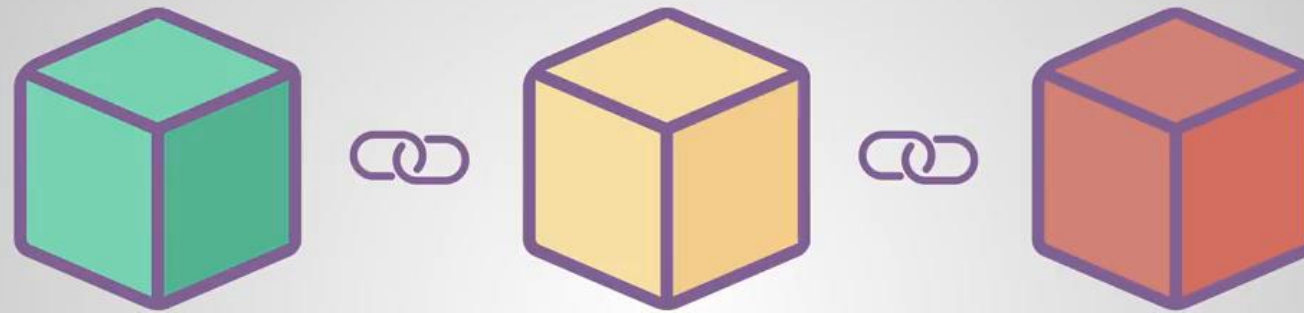
E-commerce Payment Systems

- **Blockchain** is a technology that enables organizations to create and verify transactions on a network nearly instantaneously without a central authority. Traditionally, organizations maintained their own transaction processing systems on their own databases and used this record of transactions to keep track of orders, payments, production schedules, and shipping.
- For instance, when you place an order online, it is entered into a transaction database as an order record.
- As the order works its way through the firm's factories, warehouses, shipping, and payments processes, the initial record expands to record all this information about this specific order.
- You can think of this as a *block of information* that's created for every order and that grows over time as the firm processes the order.

E-commerce Payment Systems

- A **blockchain system** is a transaction processing system that operates on a distributed and shared database rather than a single organization's database.
- The system is composed of a distributed network of computers (called a peer-to-peer [P2P] computer network).
- Unlike traditional databases, distributed ledgers are managed through a P2P architecture and do not have a centralized database.
- **Cryptocurrencies** are purely digital assets that work as a medium of exchange using blockchain technology and cryptography.
- **Bitcoin** is the most prominent example of cryptocurrency in use today.

How does a blockchain work



Blockchain

— *Simply explained* —

E-commerce Payment Systems

- Bitcoin's blockchain is maintained by hundreds of thousands of computers that are running specialized Bitcoin software. Each "block" represents a series of transactions that have been made and is protected with a cryptographic string known as a hash.
- The hash contains an encrypted timestamp and transaction data pertaining to the values of the transactions that were made, as well as a link to the previous block in the chain; but the identity of the parties to each transaction is protected.
- Because the blockchain and the ledger are maintained by so many individual users, if anyone attempts to alter the blockchain (for example, to make it seem like they have more Bitcoins than they really do), the discrepancy is quickly detected by thousands of other users and is subsequently corrected.

E-commerce Payment Systems

- In addition to being fully decentralized, Bitcoin is nearly completely anonymous.
- While anyone can view completed transactions on the blockchain, they cannot see who made the transactions or how many Bitcoins other users have.
- Executing a Bitcoin transaction does not require a name or a social security number. Instead, it merely requires a Bitcoin wallet, a simple program that allows you to store and spend Bitcoins, which are protected by encryption keys.

Review

Understand the scope of e-commerce crime and security problems, the key dimensions of e-commerce security, and the tension between security and other values.

- While the overall size of cybercrime is unclear, cybercrime against e-commerce sites is growing rapidly, the amount of losses is growing, and the management of e-commerce sites must prepare for a variety of criminal assaults.
- There are six key dimensions to e-commerce security: integrity, nonrepudiation, authenticity, confidentiality, privacy, and availability.

Review

Understand the scope of e-commerce crime and security problems, the key dimensions of e-commerce security, and the tension between security and other values.

- The more security measures that are added to an e-commerce site, the more difficult it is to use and the slower the site becomes, hampering ease of use.
- Security is purchased at the price of slowing down processors and adding significantly to data storage demands.
- Too much security can harm profitability, while not enough can potentially put a company out of business.

Review

Identify the key security threats in the e-commerce environment.

- The most common and most damaging forms of security threats to e-commerce sites include:
- ***Malicious code***—viruses, worms, ransomware, Trojan horses, and bot networks are a threat to a system's integrity and continued operation, often changing how a system functions or altering documents created using the system.
- ***Phishing***—any deceptive, online attempt by a third party to obtain confidential information for financial gain.
- ***Hacking, cybervandalism, and hacktivism***—intentionally disrupting, defacing, or even destroying a site.

Review

Identify the key security threats in the e-commerce environment.

- ***Credit card fraud/theft***—one of the most-feared occurrences and one of the main reasons more consumers do not participate in e-commerce.
- The most common cause of credit card fraud is a the systematic hacking
- ***Identity fraud***—involves the unauthorized use of another person's personal data, such as social security, driver's license, and/or credit card numbers, as well as usernames and passwords, for illegal financial benefit.
- ***Spoofing***—occurs when hackers attempt to hide their true identities or misrepresent themselves by using fake e-mail addresses or masquerading as someone else.

Identify the key security threats in the e-commerce environment

- ***Pharming***—involves redirecting a web link to an address different from the intended one, with the site masquerading as the intended destination.
- ***Sniffing***—a type of eavesdropping program that monitors information traveling over a network, enabling hackers to steal proprietary information from anywhere on a network, including e-mail messages, company files, and confidential reports.
- ***Man-in-the middle (MiTM) attack***—attack in which the attacker is able to intercept communications between two parties who believe they are directly communicating with one another, when in fact the attacker is controlling the communications.

Review

Identify the key security threats in the e-commerce environment.

- ***Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks***—hackers flood a website with useless traffic to inundate and overwhelm the network, frequently causing it to shut down and damaging a site's reputation and customer relationships.
- ***Insider attacks***—although the bulk of Internet security efforts are focused on keeping outsiders out, the biggest threat is from employees who have access to sensitive information and procedures.

Review

Describe how technology helps to secure Internet communications channels and protect networks, servers, and clients.

- **Encryption** is the process of transforming plain text or data into cipher text that cannot be read by anyone other than the sender and the receiver. Encryption can provide four of the six key dimensions of e-commerce security: message integrity, nonrepudiation, authentication, and confidentiality.
- ***Symmetric key cryptography***—Both the sender and the receiver use the same key to encrypt and decrypt a message.
- ***Public key cryptography***—Two mathematically related digital keys are used: a public key and a private key. The private key is kept secret by the owner, and the public key is widely disseminated. Both keys can be used to encrypt and decrypt a message. Once the keys are used to encrypt a message, the same keys cannot be used to unencrypt the message.

Review

Describe how technology helps to secure Internet communications channels and protect networks, servers, and clients.

- ***Public key cryptography using digital signatures and hash digests***—This method uses a mathematical algorithm called a hash function to produce a fixed-length number called a hash digest. The results of applying the hash function are sent by the sender to the recipient. Upon receipt, the recipient applies the hash function to the received message and checks to verify that the same result is produced. The sender then encrypts both the hash result and the original message using the recipient's public key, producing a single block of cipher text. To ensure both authenticity of the message and nonrepudiation, the sender encrypts the entire block of cipher text one more time using the sender's private key. This produces a digital signature or “signed” cipher text that can be sent over the Internet to ensure the confidentiality of the message and to authenticate the sender.

Review

Identify the major e-commerce payment systems in use today.

- The major types of e-commerce payment systems in use today include:
- ***Online credit card transactions***, which is the primary form of online payment system. There are five parties involved in an online credit card purchase: consumer, merchant, clearinghouse, merchant bank, and the consumer's card-issuing bank. However, the online credit card system has a number of limitations involving security, merchant risk, cost, and social equity.
- ***Alternative online payment systems***, such as PayPal, which is an online stored value payment system that permits consumers to make instant, online payments to merchants and other individuals based on the value stored in an online account.

Review

Identify the major e-commerce payment systems in use today.

- ***Mobile payment systems***, which include universal proximity wallets such as Apple Pay, Google Pay, and Samsung Pay; branded store proximity wallets such as Walmart Pay and Starbucks Pay; and P2P mobile payment apps such as Venmo, Zelle, and Square Cash.
- ***Cryptocurrencies*** based on blockchain technology, such as Bitcoin and other altcoins. Cryptocurrencies are growing in importance and can be used to hide payments from authorities as well as to support the legitimate exchange of value.

Reference

