Instructor’s Manual: Chapter 5

E-commerce Security and Payment Systems

# Learning Objectives

After reading this chapter, your students should be able to:

* 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 secure Internet communications channels and protect networks, servers, and clients.
* Appreciate the importance of policies, procedures, and laws in creating security.
* Identify the major e-commerce payment systems in use today.
* Describe the features and functionality of electronic billing presentment and payment systems.

# Key Terms

access controls, p. 306

Advanced Encryption Standard (AES), p. 292

adware, p. 272

authentication procedures, p. 306

authenticity, p. 263

authorization management system, p. 307

authorization policies, p. 307

availability, p. 264

backdoor, p. 270

BEC (business e-mail compromise) phishing, p. 273

biometrics, p. 307

black hats, p. 275

bot, p. 270

botnet, p. 270

browser parasite, p. 272

CERT Coordination Center, p. 310

certification authority (CA), p. 297

cipher text, p. 290

confidentiality, p. 263

cracker, p. 274

cybervandalism, p. 274

data breach, p. 275

Data Encryption Standard (DES), p. 292

Denial of Service (DoS) attack, p. 281

digital cash, p. 319

digital certificate, p. 297

digital envelope, p. 296

digital signature (e-signature), p. 294

Distributed Denial of Service (DDoS) attack, p. 281

drive-by download, p. 268

electronic billing presentment and payment (EBPP) system, p. 319

encryption, p. 290

exploit kit, p. 267

firewall, p. 302

grey hats, p. 275

hacker, p. 274

hacktivism, p. 274

hash function, p. 294

Heartbleed bug, 283

identity fraud, p. 279

implementation plan, p. 306

integrity, p. 263

intrusion detection system (IDS), p. 303

intrusion prevention system (IPS), p. 303

key (cipher), p. 291

malvertising, p. 268

malicious code (malware), p. 267

man-in-the-middle (MitM) attack, p. 281

merchant account, p. 313

near field communication (NFC), p. 317

nonrepudiation, p. 263

online stored value payment system, p. 315

OpenPGP, p. 298

PCI-DSS (Payment Card Industry-Data Security Standards), p. 314

pharming, p. 279

phishing, p. 272

potentially unwanted program (PUP), p. 272

Pretty Good Privacy (PGP), p. 298

privacy, p. 263

proxy server (proxy), p. 302

public key cryptography, p. 292

public key infrastructure (PKI), p. 297

ransomware (scareware), p. 269

risk assessment, p. 306

secure negotiated session, p. 299

security audit, p. 307

security organization, p. 306

security policy, p. 306

security token, p. 307

session key, p. 300

sniffer, p. 280

social engineering, p. 272

spam (junk) websites, p. 279

spoofing, p. 279

spyware, p. 272

SQL injection attack, p. 282

substitution cipher, p. 291

symmetric key cryptography (secret key cryptography), p. 291

transposition cipher, p. 291

Trojan horse, p. 269

US-CERT, p. 310

virtual currency, p. 319

virtual private network (VPN), p. 301

virus, p. 268

white hats, p. 275

worm, p. 268

WPA2, p. 301

zero-day vulnerability, p. 283

# Brief Chapter Outline

*Cyberwar: MAD 2.0*

5.1 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

5.2 Security Threats in the E-commerce Environment

Malicious Code

Potentially Unwanted Programs (PUPs)

Phishing

Hacking, Cybervandalism, and Hacktivism

Data Breaches

*Insight on Society: Equifax: Really Big Data Hacked*

Credit Card Fraud/Theft

Identity Fraud

Spoofing, Pharming, and Spam (Junk) Websites

Sniffing and Man-in-the-Middle Attacks

Denial of Service (DoS) and Distributed Denial of Service (dDoS) Attacks

Insider Attacks

Poorly Designed Software

Social Network Security Issues

Mobile Platform Security Issues

*Insight on Technology: Think Your Smartphone Is Secure?*

Cloud Security Issues

Internet of Things Security Issues

5.3 Technology Solutions

Protecting Internet Communications

Encryption

Securing Channels of Communication

Protecting Networks

Protecting Servers and Clients

5.4 Management Policies, Business Procedures, and Public Laws

A Security Plan: Management Policies

The Role of Laws and Public Policy

5.5 E-commerce Payment Systems

Online Credit Card Transactions

Alternative Online Payment Systems

Mobile Payment Systems: Your Smartphone Wallet

Social/Mobile Peer-to-Peer Payment Systems

Regulation of Mobile Wallets and Rechargeable Cards

Digital Cash and Virtual Currencies

*Insight on Business: Bitcoin*

5.6 Electronic Billing Presentment and Payment

Market Size and Growth

EBPP Business Models

5.7 Careers in E-commerce

5.8 Case Study: *The Mobile Payment Marketplace: Goat Rodeo*

5.9 Review

Key Concepts

Questions

Projects

References

# Figures

Figure 5.1 The E-commerce Security Environment, p. 262

Figure 5.2 A Typical E-commerce Transaction, p. 266

Figure 5.3 Vulnerable Points in an E-commerce Transaction, p. 267

Figure 5.4 An Example of a Nigerian Letter E-mail Scam, p. 273

Figure 5.5 Tools Available to Achieve Site Security, p. 290

Figure 5.6 Public Key Cryptography–A Simple Case, p. 293

Figure 5.7 Public Key Cryptography with Digital Signatures, p. 295

Figure 5.8 Public Key Cryptography: Creating a Digital Envelope, p. 296

Figure 5.9 Digital Certificates and Certification Authorities, p. 297

Figure 5.10 Secure Negotiated Sessions Using SSL/TLS, p. 300

Figure 5.11 Firewalls and Proxy Servers, p. 303

Figure 5.12 Developing an E-commerce Security Plan, p. 305

Figure 5.13 Alternative Payment Methods Used by U.S. Consumers, p. 312

Figure 5.14 How an Online Credit Card Transaction Works, p. 313

Figure 5.15 Mobile Wallet Adoption, p. 317

Figure 5.16 Major Players in the EBPP Marketspace, p. 323

# Tables

# Table 5.1 What’s New in E-commerce Security 2017–2018, p. 258

# Table 5.2 The Cyber Black Market for Stolen Data, p. 261

Table 5.3 Customer and Merchant Perspectives on the Different Dimensions

of E-commerce Security, p. 264

Table 5.4 Notable Examples of Malicious Code, p. 271

Table 5.5 Internet of Things Security Challenges, p. 289

Table 5.6 E-commerce Security Legislation and Regulation, p. 309

Table 5.7 Government Efforts to Regulate and Control Encryption, p. 310

Table 5.8 Major Trends in E-commerce Payments 2017–2018, p. 311

# Teaching Suggestions

This chapter first summarizes the security threats and solutions that managers of e-commerce sites need to be aware of, and then reviews the different payment systems available on the Web.

The key point students should take away from this chapter, with respect to security, is that security is a complex, multi-layered phenomenon that involves a diverse set of risks and a balanced approach. It requires three main elements: special technology, organizational rules and procedures, and laws and industry standards. A good place to start a lecture is with Figure 5.1, which illustrates the interaction and supportive nature of these three elements. No single “magic bullet” solution exists for Internet security any more than for general societal security. With respect to payment systems, the key point for students is that the Web has not created completely new methods of payment, although it has changed how methods of payment are implemented. Online consumers in the United States predominantly use credit cards for purchases, and efforts to wean consumers away from their credit cards have generally failed. The primary exception to this is PayPal, which still relies on the stored value provided by credit cards or checking accounts.

## Key Points

The opening case, *Cyberwar: MAD 2.0*, highlights the increasing vulnerability of the Web to large-scale attacks, against both “hard” targets such as physical infrastructure, as well as “soft” targets such as the U.S. political process. Ask students to discuss how their daily life might be affected as a result. Indeed, at times it appears that the Internet itself has become a battlefield involving not just rogue groups of terrorists attacking the systems of developed countries but also involving large nation states like the United States as an active participant in conducting its own cyberwar for its own purposes.

Additional questions for class discussion might include the following:

* What is the difference between cyberwar and cyberespionage?
* Why has cyberwar become more potentially devastating in the past decade?
* What damage can be done by cyberweapons like Stuxnet?
* Is it possible to find a political solution to MAD 2.0?

Section 5.1 addresses the e-commerce security environment, including the scope of the problem, including the underground economy marketplace, defining good security, the key dimensions of e-commerce security, and the tension between security and other values.

*The Scope of the Problem*. This section is likely to be of interest to students. Ask students to discuss whether they or anyone they know has ever been a victim of cybercrime. Do they think cybercrime is being overplayed or underplayed in the popular press, given the statistics available and discussed in this section?

*Defining Good Security.*Good security has many elements. Table 5.3 lists the six key ingredients required for e-commerce sites and how the key stakeholders (consumers and merchants) view the issue. You may want to walk students through this table, so they understand the nature of the problem as well as the different perspectives.

*E-commerce Security Threats.*Section 5.2 addresses the panoply of security threats in the e-commerce environment.The e-commerce environment holds threats for both consumers and merchants. Figures 5.2 and 5.3 provide illustrations of typical e-commerce transactions and vulnerable points in the transaction process. Malicious code (including exploit kits, malvertising, drive-by-downloads, viruses, worms, ransomware, Trojan horses, and bots), potentially unwanted programs (PUPs), phishing, hacking, cybervandalism and hacktivism, data breaches, credit card fraud/theft, identity fraud, spoofing/pharming, sniffing and man-in-the-middle attacks, as well as DoS/DDoS attacks are threats to e-commerce security. Credit card fraud/theft, although it appears frequently in the news, does not impact consumers as much as students might think because of federal laws that limit liability to $50 for the consumer. However, this leaves the merchant open to much higher losses. Ask students whether they have any personal experience with any of these security threats. The *Insight on Society* case, *Equifax: Really Big Data Hacked*, should be a compelling example of the potential damage to users caused by inadequate security. Questions for class discussion might include the following:

* What organization and technological failures led to the data breach at Equifax?
* What technical solutions are available to combat data breaches?
* Have you or anyone you know experienced a data breach?

Many students will not necessarily realize the relationship between poorly designed server and client software and security issues, or the security issues posed by social networks or smartphones, so this is something worth pointing out. The *Insight on Technology* case, *Think Your Smartphone Is Secure?* highlights the latter issue. Class discussion questions might include the following:

* Which mobile operating system do you think is more secure—Apple’s iOS or Google’s Android?
* What steps, if any, do you take to make your smartphone more secure?
* What qualities of apps make them a vulnerable security point in smartphone use?

As the Internet of Things grows, more of the devices and appliances around us will have components with Internet connectivity, introducing a host of new security issues. These are detailed in Table 5.5.

*Technology Solutions.*Some types of security threats can be ameliorated through technological means, but not all. Section 5.3 focuses on technology solutions for e-commerce security. A variety of encryption techniques, in particular public key encryption, are useful for protecting Internet communications; they address issues of integrity, authenticity, and confidentiality of messages. It is beneficial to walk students slowly and carefully through Figures 5.6 and 5.7 to illustrate public key encryption and digital signatures. Figure 5.9 is useful for discussing the elements of public key infrastructure. Figure 5.10 shows how SSL/TLS—the most common form of encryption used in e-commerce transactions—works. Figure 5.11 demonstrates how firewalls and proxy servers are used to protect merchant servers and networks from hackers.

There are limitations to technical security measures, and they often presume a secure organizational environment before they can work. Encryption of any kind is susceptible to disloyal or disgruntled employees and poor client-side security (such as keeping your passwords on an insecure PC directory). Encryption also slows processors and the entire transaction process; the better the security, the worse the performance.

*Policies, Procedures, and Laws.* Even the best technical security is insufficient to protect e-commerce sites. Solid organizational policies and procedures are also required, and laws, covered in Section 5.4, are needed to deter future crime by punishing e-commerce criminal behavior. Figure 5.12 illustrates the steps managers need to follow to develop a security plan. Tables 5.6 and 5.7 illustrate how the U.S. government has used laws and regulations to both impose security, while at the same time ensuring that government can read secure messages. You might ask students to evaluate the claims of the government to be able to read secure commercial messages. How can messages be secure if the government will be able to read them? Does the government have a legitimate claim here? As in all previous communications technologies, governments claim access to private messages in a variety of circumstances: war, criminal conspiracy, or imminent threats to public safety and welfare. Perhaps the real issue is who watches the government? In the United States, reliance is placed on the courts to supervise government intrusions, and on legislatures who exercise the power of the purse to control overly aggressive executive branch members.

Section 5.5 and the end-of-chapter case study focus on e-commerce payment systems. Before delving into the different types of online payment methods, you should spend a few minutes giving students a quick overview of payment systems and stakeholders. Figure 5.13 provides a list of the most popular forms of alternative online payment methods.

*Online Credit Card Transactions.*Payment by credit card is the most common form of e-commerce payment. Figure 5.14 illustrates how a typical online credit card transaction works. These transactions carry risks for merchants in particular. Moreover, credit cards are not equally distributed. Millions of U.S. citizens do not have a credit card, making it difficult for them to shop online.

*Alternative Online Payment Systems.* Other online payment methods include: online stored value payment systems such as PayPal, Pay with Amazon, Visa Checkout, Bill Me Later, mobile payment systems (see also the chapter-ending case study), digital cash, and virtual currencies.

The *Insight on Business* case, *Bitcoin*, provides a close look at this controversial form of digital cash. Questions for discussion might include:

* What are some of the benefits of using a digital currency?
* What are the risks involved to the user?
* What are the political and economic repercussions of a digital currency?
* Have you or anyone you know ever used Bitcoin?

*Electronic Billing Presentment and Payment.* EBPP systems, covered in Section 5.6, are essentially a replacement for the physical check system in the United States, which remains the dominant form of payment. Figure 5.15 provides an overview of the players in this marketplace and the different types of bill payment systems available online.

In Section 5.7, we offer students information and tips about how the concepts they’ve learned in this chapter can help them prepare for an interview for an entry-level position as a Cybersecurity Threat Management Team trainee.

The chapter-ending case study, *The Mobile Payment Marketplace: Goat Rodeo*, in Section 5.8, provides further detail on mobile payment systems.

# Case Study Questions

*1. Who are the three major players in the mobile payment market?*

The major players are the technology companies, such as Apple, Google, Samsung, PayPal, Square, and Venmo; large merchants such as Walmart, Target, and Best Buy; and the banks and credit card companies.

*2. Why is Venmo considered a social-mobile payment system?*

Venmo alerts friends to your payments if you opt in to this service.

*3. How does Apple Pay differ from Android Pay and Samsung Pay?*

Unlike Android Pay and Samsung Pay, Apple Pay does not store user funds, , but instead acts purely as an intermediary between users and their bank accounts.

*4. How does PayPal enable mobile payments?*

PayPal facilitates mobile payments in three ways: First, PayPal sells a device similar to Square that allows merchants to process credit or debit card payments using a reader plugged into another device; second, customers can use their mobile browser to make payments for purchases; and third, PayPal offers an app for mobile devices that will accept NFC payments.

**End-of-Chapter Questions**

*1. Why is it less risky to steal online? Explain some of the ways criminals deceive consumers and merchants.*

The potential for anonymity on the Internet can allow criminals to assume identities that look legitimate and at the same time shield them from law enforcement agencies. Using these assumed identities, criminals can place fraudulent orders with online merchants, intercept e-mail, steal customer information, and shut down e-commerce sites using software viruses.

*2. Explain why an e-commerce site might not want to report being the target of cybercriminals.*

E-commerce sites are often hesitant to report that they have been the targets of cybercriminals because companies fear losing the trust of consumers. The actual amount of crime is difficult to estimate because of these fears. Companies fear that if they reveal the full extent of the theft of proprietary information and financial fraud, legitimate customers will lose confidence in the e-marketing channel and will take their business offline.

*3. Give an example of security breaches as they relate to each of the six dimensions of e-commerce security. For instance, what would be a privacy incident?*

* Integrity: This is the ability to ensure that information being displayed on a website or being transmitted/received over the Internet has not been altered in any way by an unauthorized party. One type of integrity security breach would be an unauthorized person intercepting and redirecting a bank wire transfer into a different account.
* Nonrepudiation: The ability to ensure that e-commerce participants do not deny their online actions. An example of a repudiation incident would be a customer ordering merchandise online and later denying that he or she had done so. The credit card issuer will usually side with the customer because the merchant has no legally valid proof that the customer ordered the merchandise.
* Authenticity: Authenticity is the ability to identify the identity of a person or entity you are transacting with on the Internet. One instance of an authenticity security breach is “spoofing,” in which someone uses a fake e-mail address, or poses as someone else. This can also involve redirecting a web link to a different address.
* Confidentiality: The ability to ensure that messages and data are available only to authorized viewers. One type of confidentiality security breach is “sniffing,” in which a program is used to steal proprietary information on a network including e-mail messages, company files, or confidential reports.
* Privacy: The ability to control the use of personal or financial information a customer provides to an e-commerce merchant. An example of a privacy security breach is a hacker breaking into an e-commerce site and gaining access to credit card or other customer information. This violates the confidentiality of the data and also the privacy of the people who supplied the data.
* Availability: This is the ability to ensure that an e-commerce site continues to function as intended. One availability security breach is a DoS (Denial of Service) attack in which hackers flood a website with useless traffic that causes it to shut down, making it impossible for users to access the site.

*4. How would you protect your firm against a Denial of Service attack?*

One way to protect against DoS attacks would be to increase the redundancy of your network’s servers. Firewalls and proxy servers that filter communications directed at servers should also be used.

*5. Name the major points of vulnerability in a typical online transaction.*

The major points of vulnerability are at the client level, at the server level, and over the Internet communications channels.

*6. How does spoofing threaten a website’s operations?*

Spoofing can redirect customers to a knock-off website where the customers are fooled into completing an online order with a fraudulent or different company from the one with whom they intended to do business. In this way, business can be stolen away from a site. Spoof hackers can also alter orders by inflating them or changing the products ordered. The orders can then be sent on to the original site for processing and delivery. Customers will become irate at the poor customer service and will take their business elsewhere. Huge inventory fluctuations caused by these actions can also significantly harm operations.

*7. Why is adware or spyware considered to be a security threat?*

Spyware and (to a lesser degree) adware are considered as security threats because they are covertly placed on users’ computers, where they then collect and distribute private personal information. Spyware can obtain passwords, e-mail, and instant messages, and so on, whereas adware is slightly less harmful once installed.

*8. What are some of the steps a company can take to curtail cybercriminal activity from within a business?*

One measure a company can take is to implement access controls to determine which insiders can gain access to the firm’s networks. Insider access controls typically consist of login procedures using usernames, passwords, and access codes. Authorization management systems regulate where and when a user is permitted to access certain parts of a website. Entry rules are established up front for each user, and the authorization management system “knows” who is permitted to go where at all times. The authorization management system encrypts a user session and functions like a passkey following a user from page to page and only allowing access to areas where the user has been granted permission based on data that has been entered in the system database.

*9. Explain some of the modern-day flaws associated with encryption. Why is encryption not as secure today as it was earlier in the century?*

Public key encryption is computationally slow—if 128- or 256-bit keys were used to encode large documents, transmission speeds, and significant increases in processing times would occur. Symmetric key encryption is computationally faster, but requires that the sender and the receiver share the same key, which must be sent over insecure transmission lines. Encryption is also not as secure today as it was earlier in the century because computers are so much more powerful and faster that ancient means of encryption can be easily broken. Furthermore, to effectively use symmetric key encryption for commercial use today, you would need a secret key for each of the parties in a transaction: one for the bank, one for the merchant, and one for the government. Thousands of millions of keys would be needed to accommodate all e-commerce users.

*10. Briefly explain how public key cryptography works.*

Public key cryptography solves the problem of exchanging keys by creating a mathematically related public key and private key. The private key is kept secret by the owner, while the public key is widely disseminated. The main concept behind this method is that a one-way, irreversible mathematical function is used to produce the keys. Both keys can be used to encrypt and decrypt a message, but after it is encrypted, the same key cannot be used to decrypt a message. Only a person with possession of the recipient’s private key can decrypt a message. The addition of a digital signature ensures the authenticity of the message and guarantees nonrepudiation. The sender uses his or her own private key to encrypt the message along with a hash function, which has been added to create a unique digest of the message. When used with the hash function, the digital signature is even more unique than a handwritten signature. This irreversible process creates a cipher text that can be read only by the recipient using his/her private key.

*11. Compare and contrast firewalls and proxy servers and their security functions.*

Firewalls and proxy servers are used to build a wall around private networks as well as the attached servers and clients. Firewalls refer to either hardware or software that filter communication packets and prevent packets from entering the network based on a security policy. Proxy servers are software servers that handle all communications originating from or being sent to the Internet. Their primary function is to limit the access of internal clients to external Internet servers; user HTTP requests are routed to a proxy server. The user and the nature of the request must be validated before the request is sent on to the Internet. Pages sent by external Internet servers must pass through the proxy server and be deemed acceptable before they can enter the internal network and be routed to the client machine. Proxy servers also improve web performance by storing frequently used pages locally, reducing upload times, and hiding the internal network’s address so that hackers will have a difficult time monitoring the network.

*12. Is a computer with anti-virus software protected from viruses? Why or why not?*

Anti-virus software will protect a computer from many, but not all, of the most common types of viruses. The software will also destroy any viruses already present on the hard drive. However, new viruses are being developed daily, so routine updates of the software are needed to prevent new viruses from causing damage.

*13. Identify and discuss the five steps in developing an e-commerce security plan.*

The five steps in developing an e-commerce security plan are:

* Perform a risk assessment: First, an inventory of the information and knowledge assets of a company is taken, and a dollar value amount is placed on each asset. Then, this amount is multiplied by the estimated probability that the information could be compromised. This computation is used to produce a ranked list of the information assets of the firm prioritized by their value.
* Develop a security policy: A set of statements should be developed that prioritizes the information risks, identifies acceptable risk targets, and sets out the goals for achieving these targets. Included in the security policy should be a list of the personnel who are or will be entrusted with the information assets. It should also include a description of the security policies that presently exist for these assets and suggestions for improvements. Finally, it should outline the level of risk the firm is willing to accept for each asset, and the estimated cost to achieve this level of acceptable risk.
* Develop an implementation plan: The actions to achieve the security plan goals must be set out. The tools, technologies, policies, and procedures needed to achieve the acceptable levels of risk must be developed.
* Create a security organization: A security organization must be established that will train users and keep management apprised of the security threats and breakdowns. The access controls that will determine who can gain legitimate access to the firm’s networks and the authentication procedures that will be used to protect data from intruders must be determined. Authorization policies must also be established for the differing levels of access to information assets for different users.
* Perform a security audit: A security audit must be conducted to identify how outsiders are using the site and how insiders are accessing the site’s assets. A monthly report should be generated that will establish the routine and non-routine accesses to the system and identify any unusual patterns.

*14. How do biometric devices help improve security? What particular type of security breach do they reduce?*

Biometric devices help improve security by working in conjunction with digital signatures to ensure the authenticity of messages. They guarantee nonrepudiation by verifying the physical attributes of an individual. Fingerprints, retina scans, or speech recognition systems can be used to identify individuals before they are allowed to access a website or pay for merchandise with a credit card. Biometric devices also make a spoofing security breach less likely by making it more difficult for hackers to break into a site.

*15. Briefly discuss the disadvantages of credit cards as the standard for online payments. How does requiring a credit card for payment discriminate against some consumers?*

A disadvantage to credit cards is that merchants must pay a significant transaction fee of between 3% and 5% of the sale. The risks of a transaction are largely borne by the merchant. In addition to the percentage fee, merchants must also pay an additional transaction fee of $0.20 to $0.30 per transaction as well as other set-up fees. The high transaction costs make selling small items such as articles and music tracks that are paid for by credit card undesirable. Furthermore, online merchants never see the actual card being used, no card impression is taken, and no signature is available. These last three reasons are why consumers can later dispute charges. The merchant faces the risk that the transaction will be refuted and reversed even though the merchandise has already been shipped, or the digital product has already been downloaded. Existing credit card payment systems also offer poor security because neither the merchant nor the consumer can be fully authenticated. Requiring a credit card for payment also discriminates against some consumers because millions of young adults and almost 100 million Americans who cannot afford credit cards are denied access to online shopping.

*16. Describe the major steps involved in an online credit card transaction.*

The major steps involved in an online transaction are:

* The purchase
* The delivery of the order to the merchant using an SSL secure connection
* The transfer of the order to the clearinghouse over a secure line
* The verification with the consumer’s issuing bank of the availability of a balance sufficient to make the purchase
* The issuing bank crediting the merchant’s account
* A monthly statement including the charge being sent to the consumer

When a consumer wants to make a purchase, he/she first adds items to a shopping cart. Next, a secure tunnel to the Internet is created so that the consumer can send the credit card information to the merchant. Then, the merchant contacts the clearinghouse to authenticate the credit card and verify the account balance. Once the sale is approved, the issuing bank credits the merchant’s account at the merchant’s bank and finally, the debit to the consumer’s account is transmitted to the consumer in a monthly statement.

*17. Why is Bitcoin so controversial?*

Bitcoin is controversial because it is a currency that cannot be easily controlled by governments or banks. They can be used with nearly complete anonymity, and often are used for criminal or illegal purposes, which law enforcement agencies find troubling. Economists are also skeptical about Bitcoins. Users face substantial risks, including the risk that they will not attain widespread acceptance, that governments might halt their production, as well as volatility in terms of their valuation, and the potential that they may be stolen.

*18. What is NFC and how does it work?*

Near field communication (NFC)is a set of short-range wireless technologies used to share information among devices within about two inches of each other (50 mm). NFC devices are either powered or passive. A connection requires one powered unit (the initiator) and one target unpowered unit that can respond to requests from the powered unit. NFC targets can be very simple forms such as tags, stickers, key fobs, or readers. NFC peer-to-peer communication is possible where both devices are powered. An NFC-equipped smartphone, for instance, can be swiped by a merchant’s reader to record a payment wirelessly and without contact.

*19. Discuss why EBPP systems are becoming increasingly popular.*

EBPP (electronic billing presentment and payment) systems are becoming increasingly popular because of the substantial cost savings that will occur if online billing becomes the norm. The savings in postage, processing, and improved cash flow can be astounding, ranging from $0.10 to $1.50 per invoice. Furthermore, online bills can be used as a sales opportunity, providing many options for marketing and promotion such as offering rebates, and savings offers on the Web.

*20. How are the main types of EBPP systems both alike and different from each other?*

There are four EBPP business models: online banking, biller-direct, mobile, and consolidators. They are all alike because they all enable bills to be created, delivered, and paid over the Internet. However, they each go about the process in slightly different ways. To use online banking, consumers share their banking or credit card credentials with the merchant and authorize the merchant to charge the consumer’s bank account. This model has the advantage of convenience for the consumer because the payments are deducted automatically, usually with a notice from the bank or the merchant that their account has been debited. In the biller-direct model, consumers are sent bills by e-mail notification, and go to the merchant’s website to make payments using their banking credentials. This model has the advantage of allowing the merchant to engage the consumer by sending coupons or rewards. The biller-direct model is a two-step process, and less convenient for consumers. A mobile device allows consumers to make payments using mobile apps, once again relying on their bank credentials as the source of funds. Consumers are notified of a bill by text message and authorize the payment. An extension of this is the social-mobile model, where social networks like Facebook integrate payment into their messaging services. The mobile model has several advantages, not least of which is the convenience for consumers of paying bills while using their phones, but also the speed with which bills can be paid in a single step. In the consolidator model, a third party, such as a financial institution or a focused portal such as Intuit’s Paytrust, Fiserv’s MyCheckFree, Mint Bills, and others, aggregates all bills for consumers and permits one-stop bill payment. This model has the advantage of allowing consumers to see all their bills at one website or app. However, because bills come due at different times, consumers need to check their portals often. The consolidator model faces several challenges. For billers, using the consolidator model means an increased time lag between billing and payment, and also inserts an intermediary between the company and its customer.

**Projects**

1. *Imagine you are the owner of an e-commerce website. What are some of the signs that your site has been hacked? Discuss the major types of attacks you could expect to experience and the resulting damage to your site. Prepare a brief summary presentation.*

To do this project, students should supplement what they have learned in the chapter with online research to explain the clues an e-commerce owner might see to know that their site has been hacked into. Research should also supplement the student’s discussion of what types of attacks site owners should expect to experience, and the damage to the site that might result. The summary presentation should include examples of recent viruses, worms, and Trojan horses. They should provide an explanation in each instance of the damage these types of malicious code cause to the websites they infect.

1. *Given the shift toward m-commerce, do a search on m-commerce (or mobile commerce) crime. Identify and discuss the security threats this type of technology creates. Prepare a presentation outlining your vision of the new opportunities for cybercrime that m-commerce may provide.*

The purpose of this project is for students to begin to appreciate security challenges presented by wireless technology, particularly as it is increasingly being used by employees and customers to access critical enterprise data and systems. Students should consult online research sources to identify and discuss specific threats. For instance, one could integrate wireless safeguards with security processes and technologies that are already in place to protect e-business, such as enforcing passwords and selectively defining user access levels.

Some security threats the students might discuss include the fact that PC-based applications can be secured using strong authentication and encryption while developers must work with somewhat limited memory capabilities of wireless devices. This makes the use of strong authentication and encryption difficult. Another important point students might discuss is that because wireless devices such as cell phones are small and highly mobile, they are easily and frequently stolen. This means user authentication is critical for secure m-commerce. Unfortunately, experts say many current wireless protocols come up short on authentication.

1. *Find three certification authorities and compare the features of each company’s digital certificates. Provide a brief description of each company as well, including number of clients. Prepare a brief presentation of your findings.*

Students should start by conducting an online search for the names of certification authorities. Certification authorities that students might locate include, but are not limited to: VeriSign, Symantec, Entrust, GoDaddy, Digicert, GeoTrust, and IdenTrust.

Students should gather information about each company and the features of each company’s digital certificates. They should visit the company website and read the product descriptions, “About Us,” or comparable web pages. This information should be supplemented with online research in the popular business and technical press. Similar information should be garnered from two other CAs and a comparison among the three constructed.

1. *Research the challenges associated with payments across international borders and prepare a brief presentation of your findings. Do most e-commerce companies conduct business internationally? How do they protect themselves from repudiation? How do exchange rates impact online purchases? What about shipping charges? Summarize by describing the differences between a U.S. customer and an international customer who each make a purchase from a U.S. e-commerce merchant.*

Students should begin by using a search engine to find information about the challenges of conducting e-commerce globally. Although the text has repeatedly emphasized the global nature of e-commerce and its potential for easily crossing international boundaries, there are a number of obstacles, and much inter-firm coordination must take place for e-commerce firms to truly take advantage of the global marketplace.

The first challenge to international e-business is language. Companies who have taken the plunge into international e-commerce have found that simple steps such as adding a native language customer-service phone number can make sales in that country double. What holds many companies back is the price of developing a multilingual presence online. Web pages must be translated, and several different sites must be maintained, one for each country or language. It is also difficult to coordinate content and branding between the sites, and there are a myriad of business systems that must be either built or purchased. Producing a website in another language can cost from $50,000 on up and large projects can run as much as $2 million per language, but the upside is that it can quickly turn foreign browsers into buyers.

Language differences aren’t the only challenges—companies must be able to exchange financial information in a variety of currencies and account for currency fluctuations. Countries also use different formats for weights, measures, dates, telephone numbers, addresses, and other common information. Because of this an international customer might find a standard U.S. order form confusing.

Another big problem area for e-business is global trade management. Global e-commerce firms must be able to comply with a variety of complex regulations to engage in global trade. Analysts estimate that a very high percentage of international orders to U.S. e-commerce sites aren’t fulfilled because companies can’t handle the necessary procedures. Shipping goods across borders requires logistics software, yet many international shippers don’t yet have it. Furthermore, many e-businesses don’t have e-procurement software that can analyze the total “landed cost.” (“Landed cost” refers to all costs of sourcing and shipping a product internationally, including customs management, tariffs, transportation, and cost of goods.) The cost of these systems may be too steep for most small e-tailers’ budgets.

Most world cultures, especially developing nations, don’t rely on credit cards, which creates even more difficulty for international e-commerce. This is even the case in parts of Europe, Japan, Asia, South America, and much of the Middle East. Europeans generally rely on debit cards, many of which can’t be used for online transactions because their use requires a manual swipe. Forrester Research reports that few U.S. merchants offer debit/invoice payment alternatives, whereas the majority of European merchants do.

Fraud is a huge issue for merchants going global. As noted in the text, unlike the offline world where banks often take on the cost of fraudulent credit-card transactions, online merchants are typically responsible for fraudulent charges. Higher shipping and tax costs, the lack of address verification systems, and the high incidence of fraud in many Eastern European and African nations add considerable risk to any global venture. Third-party payment gateways are incorporating fraud-protection systems, but these services may increase already high per-transaction pricing without really providing the necessary protections. Address-verification services work only for cardholders living within the United States, leaving foreign transactions unchecked and at risk. As fraud has increased in sophistication in the last several years, many online firms have shut down their international transaction operations.

As far as exchange rates are concerned, most online e-commerce websites do not offer any type of currency conversion from the native sales price. This makes it extremely difficult for international customers to assess the “true” purchase price of the item. Many times, they will not know until their credit card statement arrives how much the item actually costs. For many customers, purchasing blindly in a foreign currency is a risk they won’t undertake. Very few merchants have a default currency selection system that will display the sales prices in multiple currencies. Many countries also levy import fees on goods purchased from beyond their borders. The customer can only get an idea of the initial sales price of goods, and computing the additional tariffs requires extra steps, often done manually, that can substantially affect the final purchase cost and the buyer’s decision whether to complete the transaction.

**Companion Website, Learning Tracks, and Video Cases**

You can also direct your students to the Companion Website for the book, located at [www.e-commerce2018.com](http://www.e-commerce2018.com). There they will find a collection of additional projects and exercises for each chapter; links to various technology tutorials; information on how to build a business plan and revenue models; information on careers in e-commerce, and more. Learning Tracks that provide additional coverage of various topics and a collection of video cases that integrate short videos, supporting case study material, and case study questions are also available for download from the book’s Online Instructor Resource Center at [www.pearsonhighered.com/irc](http://www.pearsonhighered.com/irc). Video Cases for this chapter include:

* Video Case 5.1 The Rise of Cyberwarfare
* Video Case 5.2 Tech Titans Clash over Future of Mobile Payments