Know all about first two pages of the Case: Cyber war: MAD (Mutually Assured Destruction) 2.0

Know what it means by ➔ “shot heard around the world”

Stuxnet, Dugu Worm, Flame, Gauss, Shamoon and more…

Know about North Korea and Cyber war.

And more only first two pages.

Common Ecommerce Security Threats & Issues

There are quite a few threats you need to protect your online store from. Let’s touch on a few common ones that often plague online businesses.

i. Financial Frauds

Financial fraud has afflicted online businesses since their inception. **Hackers make unauthorized transactions and wipe out the trail costing businesses significant amounts of losses.**

Some fraudsters also file requests for fake refunds or returns. Refund fraud is a common financial fraud where businesses refund illegally acquired products or damaged goods.

For instance, Jimmy likes to capitalize on fraudulent activities. He knows that friendly fraud is an easy medium where he can purchase an item, use it, and then refund it in order to get his money back, so he does it!

ii. Spam

Where emails are known as a strong medium for higher sales, it also remains one of the highly used mediums for spamming. Nonetheless, comments on your blog or contact forms are also an open invitation for online spammers where they leave infected links in order to harm you. They often send them via social media inbox and wait for you to click on such messages. Moreover, spamming not only affects your website’s security, but it also damages your website speed too.

iii. Phishing

It is one of the common security threats of ecommerce **where hackers masquerade as legitimate businesses and send emails to your clients to trick them into revealing their sensitive information by simply presenting them with a fake copy of your legitimate website or anything that allows the customer to believe the request is coming from the business.**

Common phishing techniques include emailing your customers or your team with fake “you must take this action” messages. This technique only works your customers follow through with the action and provide them access to their login information or other personal data which the hacker can exploit as per his benefit.

iv. Bots

An Internet **bot**, also known as a web robot, robot or simply **bot**, is a software application that runs automated tasks (scripts) over the Internet. Typically, **bots** perform tasks that are both simple and structurally repetitive, at a much higher rate than would be possible for a human alone.

You may recognize bots from your good books such as those that crawl the web and help you rank your website in Search Engine Result Pages. However, there are exclusive bots developed to scrape websites for their pricing and inventory information. The hackers use such information to change the pricing of your online store, or to garner the best-selling inventory in shopping carts, resulting in a decline in sales and revenue.

v. DDoS Attacks

Distributed Denial of Service (DDoS) attacks and DOS (Denial of Service) attacks aim to disrupt your website and affect overall sales. These attacks flood your servers with numerous requests until they succumb to them and your website crashes.

vi. Brute Force Attacks

These attacks target your online store’s admin panel in an attempt to figure out your password by brute-force. It uses programs that establish a connection to your website and use every possible combination to crack your password. You can protect yourself against such attacks by using a strong, complex password. Do remember to change it regularly.

vii. SQL Injections

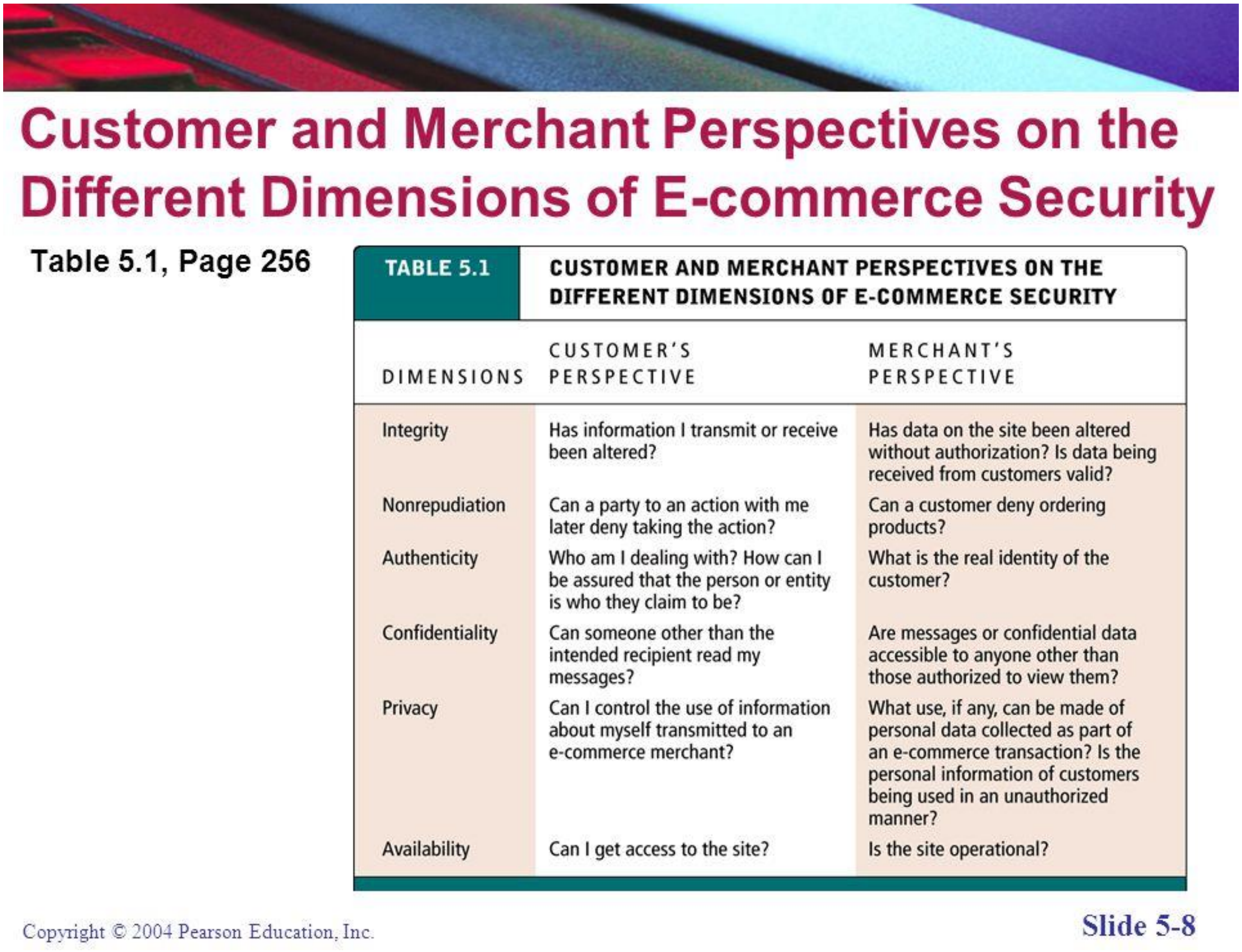
SQL injections are cyber-attacks intended to access your database by targeting your query submission forms. They inject malicious code in your database, collect the data and then delete it later on.

viii. XSS

Hackers target your website visitors by infecting your online store with malign code. You can safeguard yourself against it by implementing Content Security Policy.

ix. Trojan Horses

Admins and customers might have Trojan Horses downloaded on their systems. It is one amongst the worst network security threats where attackers use these programs to swipe sensitive information from their computers with ease.



Customer and Merchant Perspectives on the Different Dimensions of E-commerce Security

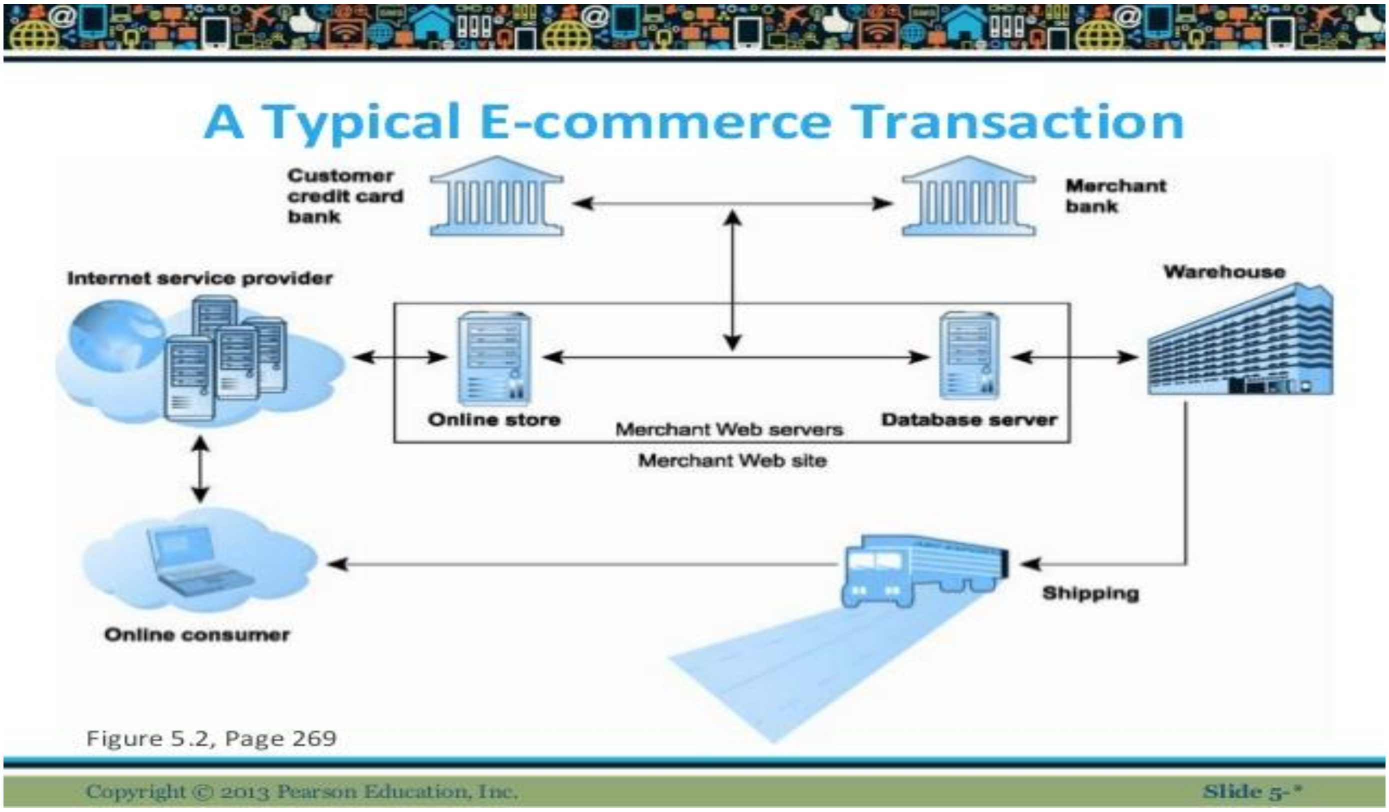
Table 5.1, Page 256

TABLE 5.1 CUSTOMER AND MERCHANT PERSPECTIVES ON THE DIFFERENT DIMENSIONS OF E-COMMERCE SECURITY

DIMENSIONS	CUSTOMER'S PERSPECTIVE	MERCHANT'S PERSPECTIVE
Integrity	Has information I transmit or receive been altered?	Has data on the site been altered without authorization? Is data being received from customers valid?
Nonrepudiation	Can a party to an action with me later deny taking the action?	Can a customer deny ordering products?
Authenticity	Who am I dealing with? How can I be assured that the person or entity is who they claim to be?	What is the real identity of the customer?
Confidentiality	Can someone other than the intended recipient read my messages?	Are messages or confidential data accessible to anyone other than those authorized to view them?
Privacy	Can I control the use of information about myself transmitted to an e-commerce merchant?	What use, if any, can be made of personal data collected as part of an e-commerce transaction? Is the personal information of customers being used in an unauthorized manner?
Availability	Can I get access to the site?	Is the site operational?

Copyright © 2004 Pearson Education, Inc.

Slide 5-8



A Typical E-commerce Transaction

Figure 5.2, Page 269

Slide 5-*

Know:

Malicious Code/Malware – includes a variety of threats such as viruses, worms, Trojan horses, and bots.

Drive-by-download – malware that comes with a downloaded file that a user requests.

Virus – a computer program that has ability to replicate or make copies of itself and spreads to other files.

Worm – malware that is designed to spread from computer to computer.

Ransomware – prevents you from accessing your computer and files and demands that you pay a fine.

Trojanhorse – apprears to be benign that does something other that expected. Often a way way virus or mailciuos codes are introduced in the computer system.

Backdoor- can be virus/worms/TH that can attack any compromised computer!

Know potentiall;y unwanted programs: (PUP):

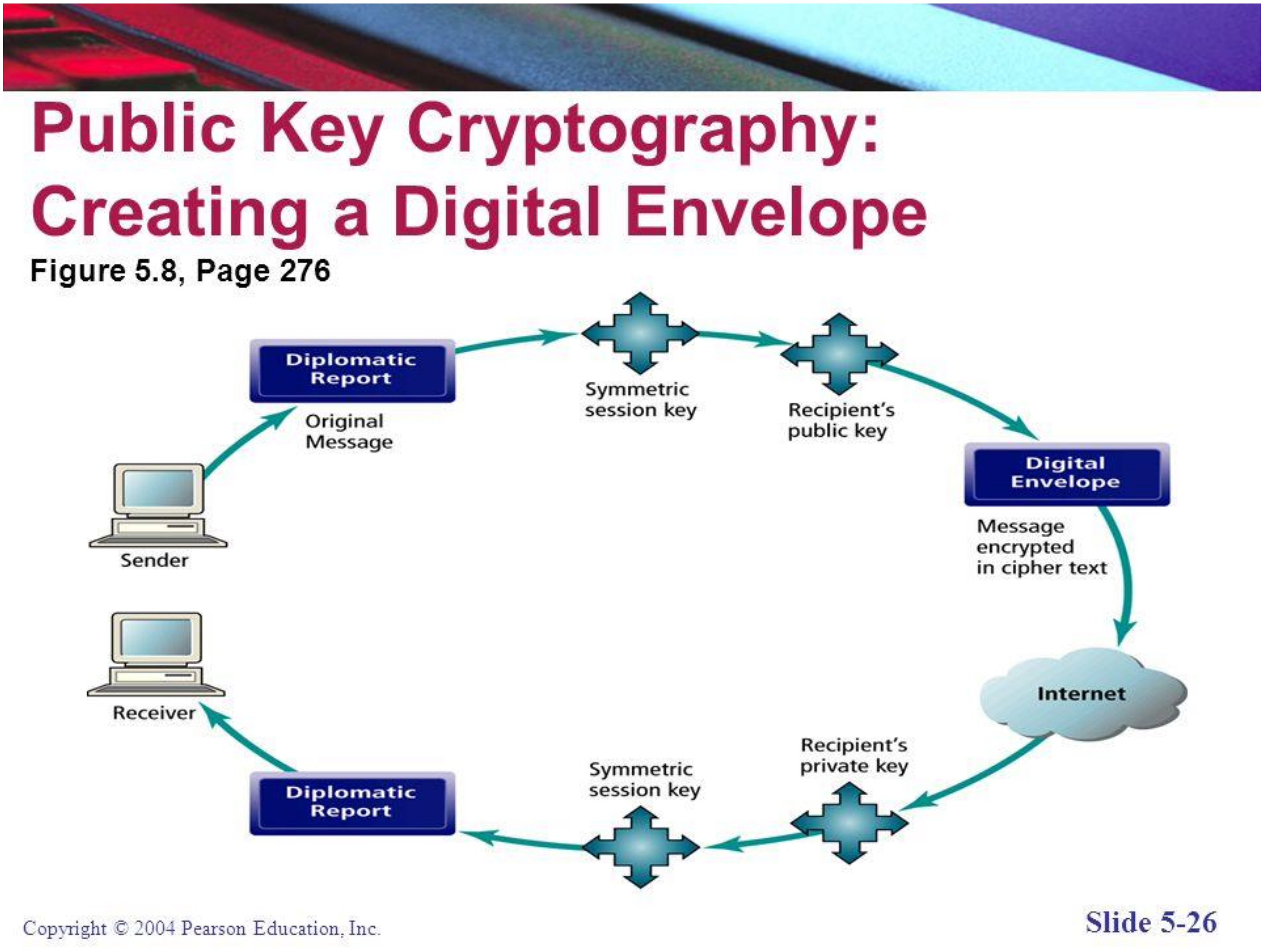
Adware- a PUP that serves pop-up ads to your computer.

Browser parasite – a program that can monitor and change of a user’s browser.

Spyware – a program used to obtain information such as users keystrokes, email, instant message, and so on.

Social engineering – exploitation f human availability and gullibility to distrinute malware.

Notabale examples of malicious codes: (see page 261)



Public Key Cryptography: Creating a Digital Envelope

Figure 5.8, Page 276

Copyright © 2004 Pearson Education, Inc.

Slide 5-26

Hacker – an individual who intends to gain unauthorized access to a computer sustem.

Cracker – within the hacking community, this term is typically used to denate a hacker with criminal intent.

Cybervandalism – intentional   disrupting. Defacing, and even destroyiong the site.

Hactivisam –

White Hats – good hackers who help to liocate and fix secuiort flaws/

Black Hats – intention to cause harm

Greay Hats – believe tha6 are persuing some greater goods by breaking in and revealing system info.

Data Breach

More will follow…