IT Security Foundations: Core Concepts

with Lisa Bock

LEARNING

Challenges for each chapter

Chapter 1. Core Security Principles

01_01. Providing a secure system

Q. One of the basic principles of providing a secure system is to manage risk and protect sensitive information. Describe what it means to ensure data confidentiality, integrity, and availability.

01_02. Keeping information safe

Q. We know there are threats to our data. Outline methods to protect data confidentiality, integrity, and availability.

01_03. Managing risk

Q. Risk is when a person, place, or thing is open or exposed to harm, which can result in injury, death, or destruction. Describe the relationship between risk, threats, and vulnerabilities.

01_04. Analyzing risk

Q. Risk analysis evaluates potential threats and system weaknesses to reduce the potential for harm. Explain what an organization can do to reduce overall risk.

01_05. Avoiding scam artists

Q. Describe ways to defend yourself against a social engineering attack.

01_06. Recognizing the Internet of Things

Q. The Internet of Things (IoT) represents a billion of devices attached to the internet. Discuss some best practice guidelines when dealing with an IoT device.

Chapter 2. Understanding Malware

02_01. Comparing malicious programs

Q. Cybercriminals use multiple methods to gain access to our data. List the main types of malware that pose a threat to our systems.

02_02. Explaining viruses and worms

Q. Outline the difference between a virus and a worm.

02_03. Eliminating unwanted surveillance

Q. Spyware can track information while you are on your device or computer and then send that information to a collection site without the user's knowledge. List the type of data collected by spyware, along with steps to defend against this threat.

02_04. Defending the OS

Q. Malware can infiltrate your system and cause a great deal of damage. Discuss some tools and apps that help defend the following operating systems:

- macOS
- Linux
- Windows

02_05. Holding data hostage

Q. Ransomware is a type of malware that holds your computer hostage until you offer some type of payment or ransom. Discuss ways someone can fall victim to a ransomware attack and how to avoid this type of threat.

Chapter 3. Breaching Your System

03_01. Stopping the impostors

Q. Describe how trojans conceal malware in order to get into your system.

03_02. Getting in the backdoor

Q. A rootkit is a collection of utilities that gets into a computer system, creates a backdoor, takes control, and remains undetected. Describe how you can get a rootkit, and what can happen once the rootkit gains access to a system.

03_03. Exploiting the unknown

Q. Explain how a zero-day attack works, along with ways to reduce the potential for this type of threat.

03_04. Challenge and response: Recognizing IoT threats

- The **Internet of Things (IoT)** poses unique challenges in managing information, as all systems are essentially interconnected.
  - In the challenge, we'll go to this website: https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/inside-the-smart-home-iot-device-threats-and-attack-scenarios
  - List five possible ways IoT devices can be attacked.

Chapter 4. Investigating Internet Security

04_01. Accessing cloud resources

Q. For many organizations and individuals, the cloud is an extension of the network. Discuss the three main types of cloud services.

04_02. Using a secure connection

Q. List three best practices to ensure a secure connection when online.

04_03. Accepting cookies

Q. Imagine you are at a picnic with friends. Someone asks, “Why do we need to accept cookies?” Explain how cookies are used while browsing a webpage.

04_04. Blocking malicious content

Q. List some steps to lock down your browser and avoid malicious activity.

04_05. Ensuring browser privacy

Q. A *secure* web browser will actively examine webpages for suspicious behavior. List some characteristics of a browser that help ensure privacy.

Chapter 5. Mobile and Wireless Security

05_01. Securing your home Wi-Fi

Q. Wireless networks send signals using radio waves, and if not properly secured, can be attacked. Outline some steps to complete when setting up your access point, can help secure wireless transmissions.

05_02. Sharing a secret

Q. One of the ways to protect your wireless traffic from prying eyes is by using a pre-shared key. When setting up your wireless router, explain the best encryption algorithm to use and why a passphrase can be a better option than a password.

05_03. Concealing your access point

Q. Explain how to reduce visibility by disabling the SSID broadcast and limit access by filtering MAC addresses to allow only registered devices to join the network.

05_04. Protecting mobile devices

Q. Today we spend a lot of time on our mobile devices. Discuss the threats to mobile devices, along with steps to secure your device.

Chapter 6. Secure Devices and Applications

06_01. Providing data confidentiality

Q. Encryption is best way to maintain confidentiality, as it scrambles data using an algorithm and a key to conceal data. Explain the difference between symmetric and asymmetric encryption.

06_02. Ensuring data integrity

Q. A hash is a one-way function used to ensure data integrity. Explain how a hash is used to ensure data integrity.

06_03. Using cryptographic techniques

Q. Outline the various services encryption provides, along with the types of applications used to secure our data.

06_04. Securing email

Q. Email is the most commonly used communication tool for personal and business use. Describe ways email can pose a risk, along with ways to secure your email.