Identify the most significant concerns for effective implementation of computer technology.

Discuss the primary privacy issues of accuracy, property, and access.

Describe the impact of large databases, private networks, the Internet, and the Web on privacy.

Discuss online identity and major laws on privacy.
Description of the security threats posed by computer criminals including employees, hackers, crackers, carders, organized crime, and terrorists.

Discuss computer crimes including creation of malicious programs such as viruses, worms, Trojan horse, and zombies as well as denial of service attacks, Internet scams, social networking risks, cyber-bullying, rogue Wi-Fi hotspots, theft, data manipulation, and other hazards.
Detail ways to protect computer security including restricting access, encrypting data, anticipating disasters, and preventing data loss.

Discuss computer ethics including copyright law, software piracy, and digital rights management as well as plagiarism and ways to identify plagiarism.
Introduction

- The ubiquitous use of computers and technology prompts some very important questions about the use of personal data and our right to privacy.
- This chapter covers issues related to the impact of technology on people and how to protect ourselves on the Web.
People

- **Privacy** – What are the threats to personal privacy and how can we protect ourselves?
- **Security** – How can access to sensitive information be controlled and how can we secure hardware and software?
- **Ethics** – How do the actions of individual users and companies affect society?
Privacy

- Privacy – concerns the collection and use of data about individuals
- Three primary privacy issues:
  - Accuracy
  - Property
  - Access
Large Databases (Page 1 of 2)

- Large organizations compile information about us.
- Federal government has over 2,000 databases.
- Telephone companies
  - Reverse directory lists of calls we make.
- Supermarkets
  - What we buy and when.
Information resellers or information brokers
- Collect and sell personal data
- Electronic profiles easily created

Personal information is a marketable commodity, which raises many issues:
- Collecting public, but personally identifying information (e.g., Google’s Street View)
- Spreading information without personal consent, leading to identity theft
- Spreading inaccurate information
  - Mistaken identity
  - Freedom of Information Act
Private Networks

- Employers can monitor e-mail legally
  - 75 percent of all businesses search employees’ electronic mail and computer files using snoopware
  - A proposed law could prohibit this type of electronic monitoring or at least require the employer to notify the employee first.
The Internet and the Web

- **Illusion of anonymity**
  - People are not concerned about privacy when surfing the Internet or when sending e-mail

- **History file** in Web browsers

- **Cookies**

- **Spyware**
Online Identity

- The information that people voluntarily post about themselves online
- Archiving and search features of the Web make it available indefinitely
Major Laws on Privacy

- Federal laws governing privacy matters have been created
  - Gramm-Leach-Bliley Act
    - Protects personal financial information
  - Health Insurance Portability and Accountability Act (HIPAA)
    - Protects medical records
  - Family Educational Rights and Privacy Act (FERPA)
    - Restricts disclosure of educational results and records
Making IT Work for You
Spyware Removal

- If you have installed any free software from the Internet this seemingly harmless software might actually be spying on you, even sending personal information to advertisers.
Security

- Threats to computer security include criminals, computer crimes, and other hazards

- Computer criminals:
  - Employees
  - Outside users
  - Hackers and crackers
  - Carders
  - Organized crime
  - Terrorists
Computer Crime (Page 1 of 3)

- Malicious Programs - Malware
  - Viruses
  - Worms
  - Trojan horse
  - Zombies
- Denial of Service
  - (DoS) attack
Computer Crime (Page 2 of 3)

- Internet scams
  - Phishing

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identity theft</td>
<td>Individual(s) pose as ISPs, bank representatives, or government agencies requesting personal information. Once obtained, criminal(s) assume a person’s identity for a variety of financial transactions.</td>
</tr>
<tr>
<td>Chain letter</td>
<td>Classic chain letter instructing recipient to send a nominal amount of money to each of five people on a list. The recipient removes the first name on the list, adds his or her name at the bottom, and mails the chain letter to five friends. This is also known as a pyramid scheme. Almost all chain letters are fraudulent and illegal.</td>
</tr>
<tr>
<td>Auction fraud</td>
<td>Merchandise is selected and payment is sent. Merchandise is never delivered.</td>
</tr>
<tr>
<td>Vacation prize</td>
<td>“Free” vacation has been awarded. Upon arrival at vacation destination, the accommodations are dreadful but can be upgraded for a fee.</td>
</tr>
<tr>
<td>Advance fee loans</td>
<td>Guaranteed low-rate loans available to almost anyone. After applicant provides personal loan-related information, the loan is granted subject to payment of an “insurance fee.”</td>
</tr>
</tbody>
</table>
Computer Crime (Page 3 of 3)

- Social networking risks
- Cyber-bullying
- Rogue Wi-Fi hotspots
- Theft
- Data manipulation
  - Computer Fraud and Abuse Act
Other Hazards

- Natural hazards
- Civil strife and terrorism
- Technological failures
- Human errors
Measures to Protect Computer Security

- Restricting access
- Encrypting data
- Anticipating disasters
  - Physical security
  - Data security
  - Disaster recovery plan
- Preventing data loss
Ethics

- Standards of moral conduct
- Copyright
  - Gives content creators the right to control the use and distribution of their work
  - Paintings, books, music, films, video games
- Software piracy
  - Unauthorized copying and distribution
  - Digital Millennium Copyright Act
  - Digital rights management (DRM)
- Plagiarism
Cryptography is the science of disguising and revealing encrypted information
- Usually refers to keeping any intercepted information private

Cryptographers are mathematicians who specialize in making and breaking codes

Annual salary is usually from $60,000 to over $100,000/year
A Look to the Future

- A Webcam on Every Corner
  - Images of public places are more accessible than ever before (e.g., Google Street View)
  - “Virtual site-seeing tours”
  - Public webcams continue to grow in popularity
Open-Ended Questions (Page 1 of 3)

- Define privacy and discuss the impact of large databases, private networks, the Internet, and the Web.
- Define and discuss online identity and the major privacy laws.
- Define security and discuss computer criminals including employees, hackers, crackers, carders, and organized crime.
Define computer crime and the impact of malicious programs, including viruses, worms, and Trojan horses, and zombies as well as cyber-bullying, denial of service, Internet scams, social networking risks, rogue Wi-Fi hotspots, theft, data manipulation, and other hazards.

Discuss ways to protect computer security including restricting access, encrypting data, anticipating disasters, and preventing data loss.
Define ethics and describe copyright law and plagiarism.