

Protecting Data and Systems

Textbook

Protecting Data and Systems

In our increasingly digital world, understanding computer security is vital. Just as we protect our homes and belongings, we must also protect our digital information and the systems that store it. This chapter explores common risks to data, different types of malicious software, and the broad impacts of cyberattacks.

Identifying Risks to Maintaining Data Confidentiality

Data confidentiality is about keeping private information secret and ensuring that only authorized individuals can access it. When confidentiality is lost, sensitive data falls into the wrong hands. Here are some common ways this can happen:

- **Shoulder Surfing:** This is a simple yet effective method where someone secretly watches you enter sensitive information. Imagine you're at an ATM, typing your PIN, or in a coffee shop, logging into your bank account on a laptop. If someone is standing behind or near you, they can easily glimpse your screen or keyboard, "surfing" over your shoulder to steal your credentials or data.
- **Illicit Access to Devices:** This risk occurs when unauthorized individuals gain direct, physical access to your devices (computers, smartphones, tablets) when they are unlocked or unattended. If your phone is left unlocked on a table, or your computer is logged in when you step away, anyone who picks it up can quickly browse your files, messages, and access your accounts, compromising your data.
- **Theft of Sensitive Items:** This refers to the physical stealing of devices or storage media that contain confidential data. This includes a stolen laptop, an external hard drive, a USB flash drive, or even documents with personal information. If these items are not properly encrypted or secured, their theft directly leads to the loss of confidentiality for the data they hold.

Viruses vs. Worms

Computer security vulnerabilities are weaknesses in software, hardware, or networks that an attacker can exploit. One common type of exploitation involves **malware**, or malicious software, which includes programs designed to cause harm. Among the most well-known types of malware are viruses and worms, which, though often confused, have a key difference in how they spread.

- **Computer Virus:** A computer virus is a type of malware that attaches itself to legitimate programs or files. Similar to a biological virus, it needs a "host" and **requires human interaction to replicate itself**. This means a virus typically spreads when a user opens an infected email attachment, clicks a malicious link, or runs an infected program. Once activated, it can then infect other files on the computer and potentially other computers if those infected files are shared.
- **Computer Worm:** A computer worm is a standalone malicious program that can **replicate itself across a network without any human interaction**. Worms exploit vulnerabilities in network software or operating systems to spread from one computer to another directly. They often scan networks for vulnerable machines, then self-replicate to those machines without the user needing to open a file or click anything. This ability to spread automatically makes worms particularly dangerous for rapidly infecting large numbers of systems.

The key distinction is replication: **a computer virus requires a user to take an action (like opening a file) for it to spread, while a computer worm can replicate autonomously across a network.**

Impacts of Computer Attacks

Computer attacks, whether from viruses, worms, or other forms of cyber threats, can have widespread and severe consequences. Evaluating these impacts involves looking at both the direct effects on computer systems and the broader social and economic effects on people.

Effects of Attacks on Computer Systems:

- **Data Loss or Corruption:** Attacks can delete, encrypt, or corrupt critical files, making them unusable. This can range from personal photos to vital business records.
- **System Downtime:** Infected systems may slow down, crash repeatedly, or become completely unusable, leading to significant disruption for individuals and organizations.
- **Compromised Functionality:** Malware can alter system settings, install unwanted software, or hijack a computer's resources for malicious purposes (e.g., turning a computer into a "bot" to launch other attacks).
- **Network Infiltration and Further Spread:** Once a system is compromised, attackers might use it as a launching pad to attack other systems within the same network, leading to a wider infection.
- **Loss of Trust in Systems:** Users may lose confidence in the reliability and security of their devices and networks, affecting their willingness to use online services.

Social and Economic Impacts on People:

- **Financial Loss:** Individuals can suffer direct financial theft through stolen banking credentials, credit card fraud, or ransomware payments. Businesses face huge costs for incident response, system recovery, legal fees, and regulatory fines.
- **Identity Theft:** Stolen personal data (Social Security numbers, birth dates, addresses) can be used by criminals to open new accounts, make fraudulent purchases, or commit other crimes in the victim's name, leading to long-term distress and financial damage.
- **Loss of Privacy:** Personal communications, health records, or sensitive personal details can be exposed, leading to embarrassment, blackmail, or exploitation.
- **Damage to Reputation:** Individuals or businesses can suffer significant reputational damage if their data is compromised or they are identified as a source of an attack.
- **Disruption of Essential Services:** Attacks on critical infrastructure (e.g., power grids, healthcare systems, transportation networks) can lead to widespread societal disruption, affecting health, safety, and daily life.
- **Job Loss:** Businesses suffering severe cyberattacks might face closures or layoffs due to financial losses, damaged reputation, or a complete inability to operate.

Understanding these vulnerabilities and potential impacts helps individuals and organizations prioritize security measures, from using strong passwords and antivirus software to implementing robust network defenses and employee training.

Critical Thinking Questions

1. Imagine you are a security consultant advising a small business. They are worried about both "shoulder surfing" and "illicit access to devices" for their employees. What are three practical, low-cost

steps you would recommend they implement immediately to protect their data confidentiality?

2. A new, very dangerous computer worm has just been released onto the internet. How might its impact on global computer networks differ significantly from a traditional computer virus, and why would it likely spread much faster?
3. Consider a scenario where a major cyberattack successfully shuts down a city's public transportation system. Beyond the immediate technical disruption, describe at least three significant social and economic impacts this would have on the city's residents and businesses over a few days.

Questions (5)

1. A person is at a coffee shop, logging into their bank account on a public Wi-Fi network. Someone standing behind them secretly watches them type their password. What type of data confidentiality risk is this?

MULTIPLE CHOICE

Choose the correct answer:

- A. Illicit Access to Devices
- B. Theft of Sensitive Items
- C. Shoulder Surfing
- D. Malware infection

2. You leave your unlocked smartphone unattended on a table in a public library. An unauthorized individual picks it up and accesses your photo gallery. Which risk to data confidentiality does this scenario illustrate?

MULTIPLE CHOICE

Choose the correct answer:

- A. Shoulder Surfing
- B. Illicit Access to Devices
- C. Theft of Sensitive Items
- D. Data Loss or Corruption

3. A user downloads an infected email attachment. When they open it, a malicious program activates and starts infecting other files on their computer. This type of malware requires human interaction to spread. What is this an example of?

MULTIPLE CHOICE

Choose the correct answer:

- A. Computer Worm
- B. Computer Virus
- C. Ransomware
- D. Spyware

4. A new, very dangerous computer worm has just been released onto the internet. How might its impact on global computer networks differ significantly from a traditional computer virus in terms of spread?

MULTIPLE CHOICE

Choose the correct answer:

- A. It requires a user to open an infected file to spread.
- B. It spreads only through physical media like USB drives.
- C. It can replicate itself autonomously across a network without human interaction.
- D. It only affects individual computers, not entire networks.

5. A small business is worried about employees' sensitive data being compromised by "shoulder surfing" and "illicit access to devices." Which of these three practical, low-cost steps would directly address these concerns?

MULTIPLE CHOICE

Choose the correct answer:

- A. Installing complex server firewalls and intrusion detection systems.
- B. Encrypting all company laptops and using multi-factor authentication for every login.
- C. Implementing mandatory lock screens, advising employees on screen privacy, and securing unattended devices.
- D. Hiring a full-time cybersecurity team for constant monitoring.

Answer Keys & Solutions

Questions

1. A person is at a coffee shop, logging into their bank account on a public Wi-Fi network. Someone standing behind them secretly watches them type their password. What type of data confidentiality risk is this?

MULTIPLE CHOICE

Correct Answer:

- | | |
|------------------------------|-------------|
| A. Illicit Access to Devices | ✗ Incorrect |
| B. Theft of Sensitive Items | ✗ Incorrect |
| C. Shoulder Surfing | ✓ Correct |
| D. Malware infection | ✗ Incorrect |

Explanation:

Consider the act of visually stealing information by looking over someone's shoulder.

2. You leave your unlocked smartphone unattended on a table in a public library. An unauthorized individual picks it up and accesses your photo gallery. Which risk to data confidentiality does this scenario illustrate?

MULTIPLE CHOICE

Correct Answer:

- | | |
|------------------------------|-------------|
| A. Shoulder Surfing | ✗ Incorrect |
| B. Illicit Access to Devices | ✓ Correct |
| C. Theft of Sensitive Items | ✗ Incorrect |
| D. Data Loss or Corruption | ✗ Incorrect |

Explanation:

Think about direct, unauthorized physical access to an unlocked device.

3. A user downloads an infected email attachment. When they open it, a malicious program activates and starts infecting other files on their computer. This type of malware requires human interaction to spread. What is this an example of?

MULTIPLE CHOICE

Correct Answer:

- A. Computer Worm ✗ Incorrect
- B. Computer Virus ✓ Correct
- C. Ransomware ✗ Incorrect
- D. Spyware ✗ Incorrect

Explanation:

Recall the malware type that attaches to legitimate programs and needs a user action to spread.

4. A new, very dangerous computer worm has just been released onto the internet. How might its impact on global computer networks differ significantly from a traditional computer virus in terms of spread?

MULTIPLE CHOICE

Correct Answer:

- A. It requires a user to open an infected file to spread. ✗ Incorrect
- B. It spreads only through physical media like USB drives. ✗ Incorrect
- C. It can replicate itself autonomously across a network without human interaction. ✓ Correct
- D. It only affects individual computers, not entire networks. ✗ Incorrect

Explanation:

Focus on the key distinction regarding replication methods for worms versus viruses.

5. A small business is worried about employees' sensitive data being compromised by "shoulder surfing" and "illicit access to devices." Which of these three practical, low-cost steps would directly address these concerns?

MULTIPLE CHOICE

Correct Answer:

- A. Installing complex server firewalls and intrusion detection systems. ✗ Incorrect

B. Encrypting all company laptops and using multi-factor authentication for every login.

✗ Incorrect

C. Implementing mandatory lock screens, advising employees on screen privacy, and securing unattended devices.

✓ Correct

D. Hiring a full-time cybersecurity team for constant monitoring.

✗ Incorrect

Explanation:

Consider simple, behavioral changes that prevent direct visual and physical access.