

Protecting Data and Systems

Textbook

Protecting Data and Systems

In our world, where more and more things are digital, it's really important to understand computer security. Just like we keep our homes and stuff safe, we also need to protect our digital information and the computer systems that hold it. This part of the book will talk about common dangers to your information, different kinds of bad computer programs, and how much damage cyberattacks can cause.

Finding Risks to Keeping Data Private

Keeping data private means making sure secret information stays secret and that only people who are allowed to see it can. When privacy is lost, sensitive information can get into the wrong hands. Here are some common ways this can happen:

Shoulder Surfing: This is a simple but effective trick where someone secretly watches you as you type in private information. Picture yourself at an ATM, typing your secret code, or at a coffee shop, logging into your bank account on your laptop. If someone is standing behind or close to you, they can easily peek at your screen or keyboard. They are "surfing" over your shoulder to steal your login details or data.

Illicit Access to Devices: This risk happens when people who aren't allowed get direct, physical access to your devices (like computers, smartphones, or tablets) when they are unlocked or left alone. 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 look through your files, messages, and get into your accounts, which puts your information at risk.

Theft of Sensitive Items: This means someone physically steals your devices or storage things that hold private data. This could be a stolen laptop, an external hard drive, a USB stick, or even papers with personal details. If these items aren't properly locked or coded, stealing them directly leads to your private data being exposed.

Viruses vs. Worms

Weaknesses in computer programs, parts, or networks that an attacker can use are called computer security vulnerabilities. A common way these weaknesses are used is through malware, which stands for malicious software. This includes programs made to cause harm. Among the most well-known types of malware are viruses and worms. Even though they are often confused, they have a key difference in how they spread.

Computer Virus: A computer virus is a type of harmful program that attaches itself to good programs or files. Like a real-life sickness, it needs a "host" and needs a person to do something for it to make copies of itself. This means a virus usually spreads when a user opens a bad email attachment, clicks on a harmful link, or runs a program that has the virus. Once it's active, it can then infect other files on the computer and possibly other computers if those infected files are shared.

Computer Worm: A computer worm is a harmful program that can make copies of itself across a network without any human help. Worms take advantage of weaknesses in network software or operating systems to spread directly from one computer to another. They often look for weak computers on networks, then copy themselves to those computers without the user needing to open a file or click anything. This ability to spread on its own makes worms especially dangerous for quickly infecting many computer systems.

The main difference is how they copy themselves: a computer virus needs a person to do something (like open a file) for it to spread, while a computer worm can spread by itself across a network.

Impacts of Computer Attacks

Computer attacks, whether they come from viruses, worms, or other online threats, can have widespread and serious effects. Figuring out these effects means looking at both what happens directly to computer systems and the bigger social and money-related effects on people.

Effects of Attacks on Computer Systems:

Data Loss or Corruption: Attacks can delete, scramble, or ruin important files, making them unusable. This can range from personal pictures to essential business records.

System Downtime: Infected systems might slow down, crash many times, or become completely unusable, causing big problems for individuals and organizations.

Compromised Functionality: Bad programs can change system settings, put unwanted software on your computer, or take over a computer's power for bad reasons (like turning a computer into a "bot" to launch other attacks).

Network Infiltration and Further Spread: Once a system is attacked, attackers might use it as a starting point to attack other systems within the same network, leading to a bigger infection.

Loss of Trust in Systems: Users might stop trusting how reliable and safe their devices and networks are, which can make them not want to use online services.

Social and Economic Impacts on People

Financial Loss: People can have money stolen directly through stolen bank details, credit card fraud, or by having to pay money to unlock their files (ransomware). Businesses face huge costs for dealing with the problem, fixing systems, legal fees, and fines.

Identity Theft: Stolen personal information (like Social Security numbers, birth dates, addresses) can be used by criminals to open new accounts, make fake purchases, or commit other crimes using the victim's name, leading to long-lasting worry and money problems.

Loss of Privacy: Personal talks, health records, or private personal details can be exposed, leading to embarrassment, blackmail, or being taken advantage of.

Damage to Reputation: Individuals or businesses can suffer serious harm to their good name if their data is exposed or if they are identified as the source of an attack.

Disruption of Essential Services: Attacks on important systems (like power grids, hospitals, transportation systems) can cause widespread problems for society, affecting health, safety, and daily life.

Job Loss: Businesses that suffer serious cyberattacks might have to close or lay off workers because of money losses, a damaged reputation, or being completely unable to operate.

Understanding these weaknesses and possible effects helps individuals and organizations decide to focus on security measures. This can include using strong passwords and antivirus programs, as well as setting up strong network defenses and training employees.

Critical Thinking Questions

1. Imagine you are a security expert giving advice to a small business. They are worried about their employees' data privacy because of "shoulder surfing" and "illicit access to devices." What are three simple and cheap things you would tell them to do right away to protect their data?
2. A very dangerous new computer worm has just been released online. How might its effect on computer networks around the world be very different from a regular computer virus, and why would it likely spread much faster?
3. Think about a situation where a major cyberattack successfully shuts down a city's public transportation system. Besides the immediate technical problems, describe at least three big social and money-related effects 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.