

Security and Privacy

Textbook

Security and Privacy



Computer networks and the internet are essential, but they come with security and privacy risks. This guide helps you understand and protect your information.

Security and Privacy in Computer Networks

When you're online, you're on computer networks that share information globally. While useful, these networks also have big security concerns. Network security means protecting data from threats like unauthorized access, data breaches, malware (viruses), and Denial-of-Service (DoS) attacks.

Privacy in networks is about controlling your personal information. Websites and apps collect data about your online activities, raising questions about its use. Your online identity forms a permanent "digital footprint," affecting your reputation. It's often unclear how your data is collected and used.

Online Identity and Privacy: What's Your Digital Footprint?

Your online identity is your digital self (social media, emails, posts). Managing it is crucial because it's public, permanent, and shapes perceptions.

To protect your privacy: think before you post, adjust privacy settings, be cautious of excessive information requests, use strong, unique passwords (consider a password manager), enable two-factor authentication (2FA), be careful on public Wi-Fi, and regularly review your digital footprint.

Investigating Ransomware Attacks

Ransomware is malicious software that encrypts files or locks your computer, demanding a ransom for access. It spreads through phishing emails, malicious websites, outdated software, or harmful ads.

Ransomware causes data loss, financial costs, reputational damage, and service disruptions. To prevent it: back up files regularly, keep software updated, use antivirus/anti-malware software, and be cautious with unknown emails/links. Education on ransomware is your best defense.

Exploring Access Control Rules

Access control rules secure computer systems by defining who can access resources and what they can do. Authentication verifies identity (usernames/passwords), authorization determines actions, and accountability tracks user activity.

Models include: Discretionary Access Control (DAC) (owner grants access, less secure in large groups), Mandatory Access Control (MAC) (strict, high-security, based on labels), and Role-Based Access Control (RBAC) (common, permissions by role). Access control is vital for data protection, system integrity, compliance, and risk reduction.

Security and Temporary Storage

Programs use temporary storage like RAM or temporary files. This data is often volatile. Memory safety vulnerabilities, like buffer overflows, can occur if programs mishandle this storage, letting attackers inject harmful code. Insecure temporary files on disk also pose risks. Secure handling of all data, even temporary, is essential.

Online Safety

Staying safe online is critical due to dangers in direct electronic communication (email, chat, social media DMs). Malicious actors use these platforms for cyberbullying, harassment, grooming, and can lead to real-world harm like human trafficking. These channels also spread phishing scams, leading to identity theft or financial fraud. Exercise extreme caution and verify identities.

Evaluating Risks to Personal Information Online

Internet use risks your personal information, especially with insecure websites/software that might share your data without consent. The worst outcome is theft of personal data (SSN, banking info, identity), leading to fraud.

For example, John used a questionable gaming site and later faced spam and missing bank funds, indicating data compromise. He should contact his bank immediately, cancel his card, change passwords (enabling 2FA), scan for malware, and avoid/report such sites.

The Impact of Permissible Privacy and Security

"Permissible privacy and security" refers to user control over online information and settings. This includes account settings, cookies, and application permissions, all impacting digital safety.

Managing account settings limits data exposure. Cookies track Browse; manage them to control tracking. Application permissions control app access to your data (location, contacts). Understanding and using these settings helps control your digital footprint, reducing vulnerability and protecting privacy. Ignoring them increases risk.

Conclusion

Understanding security and privacy is essential in the digital world. Being aware of your online identity, ransomware threats, and access control makes you a responsible and secure digital citizen.

Critical Thinking Questions

1. Imagine a student uses a photo editing app that asks for permission to access their microphone and camera, even though the app's main purpose is just to edit photos. What are the potential security risks associated with granting these unnecessary permissions? What steps could the student take to evaluate if these permissions are truly needed before granting them?
2. A company's employee accidentally clicks on a suspicious link in an email, which leads to a malware infection that spreads across the company's internal network. Discuss how this incident could impact the company's operations, its customers' trust, and potentially lead to legal issues. What

responsibilities does the company have to prevent such incidents, and what actions should they take after such a breach?

3. Consider the concept of a "digital footprint." How might a positive or negative digital footprint impact a person's future opportunities, such as college admissions or job applications? What advice would you give to someone who wants to build a strong, positive digital footprint while still maintaining their personal privacy?

Questions (5)

1. A user's computer suddenly displays a message stating that all their files have been encrypted, and they must pay a ransom in cryptocurrency to get them back. What type of malicious software has infected their computer?

MULTIPLE CHOICE

Choose the correct answer:

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

2. A high school student posts a photo online that inadvertently shows their school ID, including their full name and student ID number. What is a potential negative consequence of this action, related to their "digital footprint"?

MULTIPLE CHOICE

Choose the correct answer:

- A. The photo will automatically be deleted by the platform.
- B. The information is now part of their permanent online identity and could be misused for identity theft or targeted scams.
- C. The school will immediately issue them a new, more secure ID.
- D. The photo will only be visible to their close friends.

3. Which of the following actions is a key defense against ransomware attacks, as recommended in the passage?

MULTIPLE CHOICE

Choose the correct answer:

- A. Regularly deleting all files from your computer to prevent encryption.
- B. Keeping all software outdated to avoid new vulnerabilities.
- C. Regularly backing up your files to external drives or cloud storage.
- D. Clicking on all links from unknown senders to test their safety.

4. A system administrator is setting up access for new employees. They want to simplify management by assigning permissions based on job roles (e.g., "Manager," "Staff," "Intern"). Which access control model would be most appropriate for this organizational s

MULTIPLE CHOICE

Choose the correct answer:

- A. Discretionary Access Control (DAC)
- B. Mandatory Access Control (MAC)
- C. Role-Based Access Control (RBAC)
- D. Least Privilege

5. You are worried about websites collecting data about your online activities and building profiles of your behavior. Which feature can you manage or block to control this tracking?

MULTIPLE CHOICE

Choose the correct answer:

- A. Account settings
- B. Passwords
- C. Cookies
- D. Two-factor authentication

Answer Keys & Solutions

Questions

1. A user's computer suddenly displays a message stating that all their files have been encrypted, and they must pay a ransom in cryptocurrency to get them back. What type of malicious software has infected their computer?

MULTIPLE CHOICE

Correct Answer:

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

Explanation:

Recall the malware type that encrypts files and demands payment.

2. A high school student posts a photo online that inadvertently shows their school ID, including their full name and student ID number. What is a potential negative consequence of this action, related to their "digital footprint"?

MULTIPLE CHOICE

Correct Answer:

- | | |
|--|-------------|
| A. The photo will automatically be deleted by the platform. | ✗ Incorrect |
| B. The information is now part of their permanent online identity and could be misused for identity theft or targeted scams. | ✓ Correct |
| C. The school will immediately issue them a new, more secure ID. | ✗ Incorrect |
| D. The photo will only be visible to their close friends. | ✗ Incorrect |

Explanation:

Think about the long-term impact and public nature of online content.

3. Which of the following actions is a key defense against ransomware attacks, as recommended in the passage?

MULTIPLE CHOICE

Correct Answer:

- A. Regularly deleting all files from your computer to prevent encryption. ✗ Incorrect
- B. Keeping all software outdated to avoid new vulnerabilities. ✗ Incorrect
- C. Regularly backing up your files to external drives or cloud storage. ✓ Correct
- D. Clicking on all links from unknown senders to test their safety. ✗ Incorrect

Explanation:

Consider the most effective way to recover your data if it's encrypted.

4. A system administrator is setting up access for new employees. They want to simplify management by assigning permissions based on job roles (e.g., "Manager," "Staff," "Intern"). Which access control model would be most appropriate for this organization's

MULTIPLE CHOICE

Correct Answer:

- A. Discretionary Access Control (DAC) ✗ Incorrect
- B. Mandatory Access Control (MAC) ✗ Incorrect
- C. Role-Based Access Control (RBAC) ✓ Correct
- D. Least Privilege ✗ Incorrect

Explanation:

Think about the model that assigns permissions to groups based on their function.

5. You are worried about websites collecting data about your online activities and building profiles of your behavior. Which feature can you manage or block to control this tracking?

MULTIPLE CHOICE

Correct Answer:

A. Account settings

✗ Incorrect

B. Passwords

✗ Incorrect

C. Cookies

✓ Correct

D. Two-factor authentication

✗ Incorrect

Explanation:

Recall the small files websites use to track your Browse habits.