

Security and Privacy

Textbook

Security and Privacy



In our interconnected world, computers and networks are vital. We use the internet for everything from entertainment to essential services. However, this digital reliance comes with security and privacy risks. This chapter will help you understand these challenges and protect your information in the digital landscape.

Security and Privacy in Computer Networks

When you go online, you're using computer networks, which allow global information sharing. While beneficial, these networks have significant security and privacy concerns. Network security protects data and systems from threats like unauthorized access, where people gain entry without permission to steal data. Data breaches involve the accidental or intentional release of private information. Malware infections, such as viruses, disrupt operations or steal data, while Denial-of-Service (DoS) attacks overwhelm systems to make them unavailable.

Privacy in networks means controlling your personal information. Websites and apps extensively collect data about your online activities, raising questions about its use and access. Your online identity and the permanency of data mean everything you share online forms a "digital footprint" that's hard to erase, impacting your reputation long-term. Also, a lack of transparency often makes it difficult to understand how your data is collected and used by various online entities.

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

Your online identity is your digital persona, including social media, emails, and posts. It's crucial to manage it because it can become public, is surprisingly permanent, and shapes perceptions from potential employers to new friends.

To protect your online privacy: think before you post, as online content is hard to retract. Adjust privacy settings on all accounts to limit visibility. Be cautious of websites asking for excessive personal information. Use strong, unique passwords and consider a password manager. Enable two-factor authentication (2FA) for added security. Be careful on public Wi-Fi, avoiding sensitive transactions due to security risks. Finally, regularly review your digital footprint by searching for your name online.

Investigating Ransomware Attacks

Ransomware is a malicious software that encrypts your files or locks your computer, demanding a ransom (often cryptocurrency) for access or decryption. If you don't pay, files may be lost.

Ransomware often spreads through phishing emails with malicious attachments or links, visits to malicious websites, or by exploiting software vulnerabilities in outdated programs. It can also spread via malvertising.

The impact of ransomware is severe, leading to data loss if decryption fails, significant financial costs from ransom payments and recovery, reputational damage for businesses, and disruption of services in critical sectors like healthcare.

To prevent ransomware: regularly back up your files to external drives or cloud storage. Keep all software updated to patch security flaws. Use and update antivirus/anti-malware software. Be highly cautious with emails and links from unknown senders. Your best defense is to educate yourself on how ransomware operates.

Exploring Access Control Rules

Access control rules are vital for securing computer systems, defining who can access what resources and what actions they can perform. Authentication verifies identity, typically with usernames and passwords. Authorization then determines what authenticated users can do. Accountability tracks user actions for auditing.

There are different access control models. Discretionary Access Control (DAC) allows resource owners to grant or deny access, but can be less secure in large organizations. Mandatory Access Control (MAC) is stricter, used in high-security environments, where access is based on predefined security labels for users and resources, and users can't override these rules. Role-Based Access Control (RBAC) is common in organizations; permissions are assigned to specific "roles" (e.g., "Student," "Teacher"), and users inherit permissions by being assigned to these roles, simplifying management.

Access control is crucial for data protection, preventing unauthorized access to sensitive information. It ensures system integrity by allowing only authorized users to modify critical files. It also helps organizations meet compliance standards and reduces risk from insider threats and external attacks.

Security and Temporary Storage

Programs use temporary storage like RAM or temporary files to hold data during execution. However, this storage is often volatile; data in RAM disappears when the program closes, creating a risk for unpersisted information. Memory safety vulnerabilities, like buffer overflows, can occur if programs mishandle this storage, potentially allowing attackers to inject malicious code, leading to system compromise. Similarly, insecure temporary files on disk could be accessed or tampered with by others, introducing further security risks. These issues highlight the critical need for secure handling of all data, even temporary data.

Online Safety

Staying safe online is critical, as many digital interactions can pose serious dangers to an individual's safety and security.

One major area of risk lies in direct electronic communication, such as email, chat rooms, instant messaging, and even social media direct messages. These platforms can be exploited by malicious actors for various forms of predatory behavior, including cyberbullying, harassment, and grooming. Predators often use these channels to build trust over time, collecting personal information and manipulating victims.

This can tragically escalate to severe real-world harm where individuals are lured into dangerous situations under false pretenses. Beyond direct threats, these communication methods are also common vectors for phishing scams, where deceptive messages attempt to trick individuals into revealing personal information

or downloading malware, which can lead to identity theft or financial fraud. Therefore, exercising extreme caution, verifying identities, and being aware of the content shared in all forms of direct electronic communication are essential for personal safety online.

Evaluating Risks to Personal Information Online

Accessing the Internet poses risks to your personal information, especially with websites or software lacking strong security. Many platforms don't protect against sharing your personal data, meaning your information could be exposed without consent.

The worst outcome is theft of personal data, including Social Security numbers, banking information, and your identity. This stolen data can lead to financial fraud and other illegal activities, causing major distress.

Consider John, who used a questionable gaming website. The next morning, he had spam emails and missing money from his bank. What likely happened is the website either directly stole his data or was hacked. The spam shows his email was exposed, and the missing money indicates compromised banking details.

John should immediately contact his bank, cancel his card, and change passwords for his email and any other accounts using the same password, enabling two-factor authentication. He should also scan his computer for malware and avoid such sites in the future, reporting the website if possible.

The Impact of Permissible Privacy and Security

"Permissible privacy and security" refers to how much control users have over their information and security settings online. This includes account settings, cookies, and app permissions, all impacting your digital safety.

Account settings let you control who sees your online posts and details. Managing these limits exposure to unwanted attention or data theft. Leaving default settings often grants more access than intended.

Cookies track Browse habits. While some are useful, third-party cookies can build detailed profiles of your online behavior. You can manage or block cookies to control this tracking.

Application permissions on devices control what an app can access (e.g., location, contacts). Granting too many permissions exposes sensitive data to developers or, if the app is malicious, to others. Understanding and using these settings lets you control your digital footprint, reducing vulnerability and protecting privacy. Ignoring them can lead to unwanted data sharing and increased risk.

Conclusion

As you navigate the digital world, understanding security and privacy is essential. By being aware of your online identity, recognizing ransomware threats, and appreciating access control, you become a more responsible and secure digital citizen.

Critical Thinking Questions

1. Imagine a high school student posts an innocent photo online that reveals a sensitive detail (like a school ID or street sign). Describe the potential negative consequences and suggest three proactive steps the student could have taken to prevent these issues.
2. A local hospital suffers a ransomware attack, encrypting patient records. Discuss the immediate and long-term impacts on the hospital, its patients, and the community. What ethical considerations arise concerning paying the ransom for a vital service like healthcare?
3. Considering DAC, MAC, and RBAC, propose a unique real-world scenario for each where it would be the most appropriate choice. Explain why each model fits its scenario best and its limitations in other contexts.

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.