

Class 7 Computer

Chapter 4

Ethics and Safety Measures in Computing

Complete Questions and Answers

A. LET'S WORKOUT – ANSWERS

A. Tick (✓) the correct option.

1. Which of the following refers to the illegal distribution of software?

- a. Cookie
- b. Hacking
- c. Spam
- d. **Software Piracy ✓**

Answer: d. Software Piracy

2. _____ is a trace that someone leaves while using the Internet.

- a. Digital Media
- b. Digital Statement
- c. **Digital Footprint ✓**
- d. Digital Information

Answer: c. Digital Footprint

3. _____ is the process of stealing information through the Internet.

- a. Cracking
- b. **Phishing ✓**
- c. Hacking
- d. Plagiarism

Answer: b. Phishing

Note: The chapter's definition specifically describes phishing as a cybercrime involving false e-mails and attempts to obtain personal/financial information.

4. Which of the following refers to harassing a person using Internet?

- a. Social Networking
- b. **Cyberbullying ✓**
- c. Hacking
- d. Spamming

Answer: b. Cyberbullying

5. Which of the following symbols helps you to assure that a website is safe?

- a. Key symbol
- b. **Lock symbol ✓**
- c. Shield symbol
- d. All of these

Answer: b. Lock symbol

B. FILL IN THE BLANKS

1. _____ is the act of taking someone else's work and passing them as their own.

Answer: Plagiarism

2. _____ refers to a software or a network device that acts as a wall between the computer and the network.

Answer: Firewall

3. _____ Property Rights gives the creator the complete right over their product.

Answer: Intellectual

4. _____ refers to the safety measures while using the Internet.

Answer: Cybersecurity

5. A person must follow some guidelines while using the Internet, known as _____.

Answer: Netiquettes

C. TRUE OR FALSE

1. Internet is the biggest network of computers connected all over the world.

Answer: True (T)

2. Cyberbullying refers to attack or harass a person online.

Answer: True (T)

3. Illegal way of copying and sharing a software is known as plagiarism.

Answer: False (F)

It is known as software piracy.

4. Keep changing your passwords regularly.

Answer: True (T)

5. Computer ethics are common guidelines that a person must follow while using a computer.

Answer: True (T)

D. ANSWER THE FOLLOWING

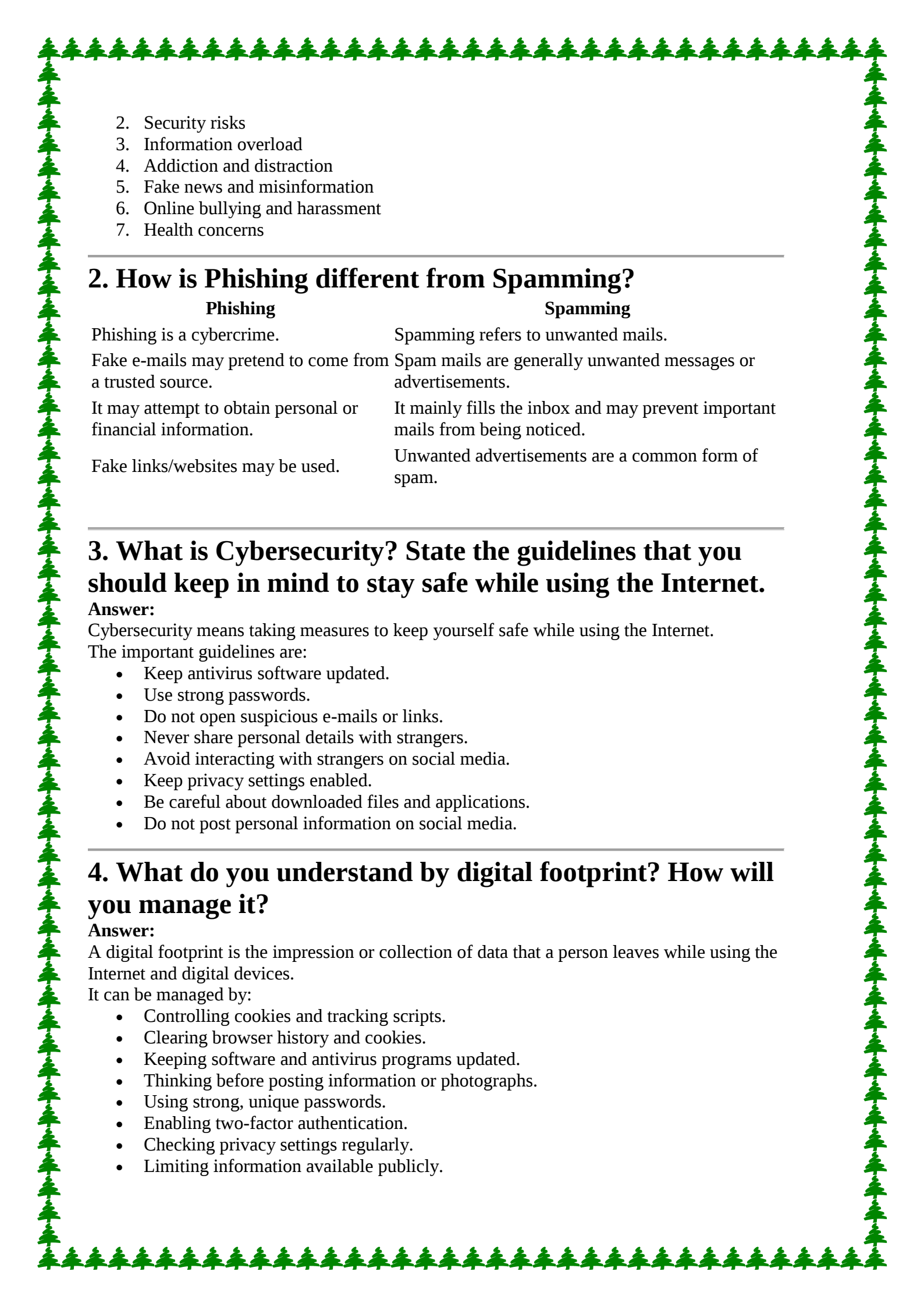
1. Write any five advantages and disadvantages of the Internet.

Advantages:

1. Lots of information
2. Online services
3. Business promotion
4. E-learning
5. Entertainment
6. Discussion forums
7. Alternative communication

Disadvantages:

1. Privacy concerns

- 
2. Security risks
 3. Information overload
 4. Addiction and distraction
 5. Fake news and misinformation
 6. Online bullying and harassment
 7. Health concerns

2. How is Phishing different from Spamming?

Phishing

Phishing is a cybercrime.

Fake e-mails may pretend to come from a trusted source.

It may attempt to obtain personal or financial information.

Fake links/websites may be used.

Spamming

Spamming refers to unwanted mails.

Spam mails are generally unwanted messages or advertisements.

It mainly fills the inbox and may prevent important mails from being noticed.

Unwanted advertisements are a common form of spam.

3. What is Cybersecurity? State the guidelines that you should keep in mind to stay safe while using the Internet.

Answer:

Cybersecurity means taking measures to keep yourself safe while using the Internet.

The important guidelines are:

- Keep antivirus software updated.
- Use strong passwords.
- Do not open suspicious e-mails or links.
- Never share personal details with strangers.
- Avoid interacting with strangers on social media.
- Keep privacy settings enabled.
- Be careful about downloaded files and applications.
- Do not post personal information on social media.

4. What do you understand by digital footprint? How will you manage it?

Answer:

A digital footprint is the impression or collection of data that a person leaves while using the Internet and digital devices.

It can be managed by:

- Controlling cookies and tracking scripts.
- Clearing browser history and cookies.
- Keeping software and antivirus programs updated.
- Thinking before posting information or photographs.
- Using strong, unique passwords.
- Enabling two-factor authentication.
- Checking privacy settings regularly.
- Limiting information available publicly.

- Using a pseudonym for suitable online activities.

5. How does someone violate a person's intellectual property rights? Explain with an example.

Answer:

A person's intellectual property rights are violated when someone uses, copies, distributes, performs or displays their copyrighted work without permission or a valid licence.

Example:

If a student copies another person's copyrighted artwork and uploads or sells it as their own without permission, it is a violation of intellectual property rights.

6. SHORT NOTES

1. Firewalls

A firewall is a network security measure that monitors and controls network traffic according to predefined rules. It acts as a barrier to protect a network from unauthorised access and unwanted traffic. Firewalls may be hardware-based or software-based.

2. Hacking

Hacking is gaining access to a victim's computer for the purpose of stealing information. To reduce the risk of hacking, users should use strong passwords, update their computers, avoid untrusted USB devices and public networks, and download applications only from trusted sources.

3. Software Piracy

Software piracy is the illegal copying, distributing, sharing, selling or use of software. It can be prevented by purchasing software from authorised sources, avoiding unauthorised software and registering software after purchasing or downloading it.

4. Netiquettes

Netiquettes are rules and guidelines for behaving politely and responsibly on the Internet. They include being respectful, thinking before posting, protecting personal information, respecting privacy and copyright, following e-mail etiquette and staying safe online.

5. Cyberbullying

Cyberbullying is attacking or harassing a person through the Internet. Examples include insulting someone through messages, making fun of someone, sharing private information without permission and blackmailing. It can be avoided by protecting personal information, avoiding unknown people online and informing elders about bullying.

QUICK REVISION – ONE-LINE QUESTIONS

Question	Answer
What is the biggest network of computers?	Internet
What is Internet Etiquette called?	Netiquette
What are guidelines for proper computer use called?	Computer ethics

Question	Answer
What is taking another person's work and presenting it as one's own?	Plagiarism
What is online harassment called?	Cyberbullying
What is a fake message pretending to be from a trusted source?	Phishing
What is gaining access to a computer to steal information?	Hacking
What are unwanted e-mails called?	Spam
What is illegal copying/distribution of software called?	Software piracy
What protects an original creator's work?	Intellectual Property Rights
What keeps users safe while using the Internet?	Cybersecurity
What acts as a wall between a computer/network and unwanted traffic?	Firewall
What is the trace left by a person while using the Internet?	Digital footprint
What symbol indicates a secure website in the chapter?	Lock symbol
What authentication method is recommended for better account security?	Two-factor authentication

=====*****=====

A. LET'S GET READY

Tick (✓) the action if it is justified and cross (X) if it is not.

1. Ankur was writing an e-mail. He left his seat for a while. Meanwhile, his sister came to his seat and read the letter.

Answer: X Not justified.

Ankur's sister should not read his e-mail without his permission because it violates his privacy.

2. Without the knowledge of her parents, Seema bought a game online using her parent's credit card.

Answer: X Not justified.

Seema should not use her parents' credit card without their knowledge and permission.

3. Raj is working on his father's laptop, but he never opens his father's files or e-mails.

Answer: ✓ Justified.

Raj respects his father's privacy by not opening his personal files or e-mails.

4. Vikram is listening to songs loudly on speakers while his sister is preparing for her exams in the same room.

Answer: X Not justified.

He should consider his sister's needs and avoid disturbing her while she is studying.

5. Ritu sets a unique password for her e-mail account and changes it every month.

Answer: ✓ Justified.

Using a strong, unique password and changing it regularly helps protect an account from unauthorised access.

B. MYTHS & FACTS

1. A person should always respect other's privacy.

Answer: Fact ✓

2. A person should share personal details on the Internet.

Answer: Myth ✗

3. A person can use another's computer without asking for permission.

Answer: Myth ✗

4. A person should never download any software from an illegal resource.

Answer: Fact ✓

C. IMPORTANT QUESTIONS AND ANSWERS FROM THE CHAPTER

1. What is the Internet?

Answer:

The Internet is one of the biggest networks of computers. It consists of computers from all over the world and allows people to access information and communicate with one another.

2. Write any five advantages of the Internet.

Answer:

The five advantages of the Internet are:

1. It provides access to a vast amount of information.
2. It provides online services such as e-mail, chatting and video conferencing.
3. It helps in promoting businesses.
4. It supports e-learning.
5. It provides entertainment and communication facilities.

Other advantages mentioned in the chapter include discussion forums and alternative communication methods.

3. What are the disadvantages of the Internet?

Answer:

Some disadvantages of the Internet are:

1. Privacy concerns
2. Security risks
3. Information overload
4. Addiction and distraction
5. Fake news and misinformation
6. Online bullying and harassment
7. Health concerns

Excessive Internet use can also cause physical problems such as eye strain, obesity and sleep disturbances.

4. What are Computer Ethics?

Answer:

Computer ethics are the social and moral guidelines that a person should follow while using computers.

5. Write any five guidelines of Computer Ethics.

Answer:

1. **Privacy and Data Protection** – Respect other people's privacy and protect personal data.
 2. **Environmental Responsibility** – Minimise energy consumption and e-waste.
 3. **Copyright** – Respect copyrights, trademarks and other people's work.
 4. **Health Factor** – Maintain balanced screen time along with physical activities.
 5. **Illegal Practices** – Do not download, install or use software without a proper licence.
-

D. NETIQUETTES

6. What is Netiquette?

Answer:

Netiquette stands for **Internet Etiquette**. It is a set of rules and guidelines for behaving politely and responsibly online.

7. Write any five Netiquettes.

Answer:

1. Be respectful to others online.
 2. Think before posting anything.
 3. Protect personal information.
 4. Respect other people's privacy.
 5. Follow proper e-mail etiquette.
 6. Respect copyright.
 7. Stay safe and report anything suspicious to a trusted adult.
-

E. CYBERCRIME

8. What is cybercrime?

Answer:

Cybercrime is a criminal act carried out with the help of a computer or the Internet. Examples include hacking, phishing, identity theft, online fraud, cyberbullying, online stalking and harassment.

9. What is plagiarism?

Answer:

Plagiarism is the act of taking someone else's work and presenting it as one's own.

How can plagiarism be prevented?

1. Always mention the source of the information.
 2. Use quotation marks for statements said by someone else.
 3. Read and understand the content and then rewrite it in your own words.
-

10. What is cyberbullying?

Answer:

Cyberbullying is a method of attacking or harassing a person using the Internet. It is also called online bullying.

Examples of cyberbullying:

- Making fun of someone to hurt them emotionally.
 - Sending insulting or inappropriate texts or e-mails.
 - Posting someone's private information without consent.
 - Blackmailing others online
-

11. How can cyberbullying be avoided?

Answer:

1. Never trust people online unless you know them personally.
 2. Never disclose personal information such as your address or phone number.
 3. Do not interact beyond a healthy limit with people you do not know.
 4. Tell your elders if you are being bullied or see someone being bullied.
-

F. PHISHING

12. What is phishing?

Answer:

Phishing is a cybercrime in which false e-mails are sent to a victim pretending to be from a trusted source. Such e-mails may contain links to fake websites designed to obtain personal or financial information.

13. How can phishing be avoided?

Answer:

1. Check the sender's name and the subject before opening an e-mail.
 2. Check the website address before entering information.
 3. Look for the lock symbol indicating a secure website.
 4. Verify a website before entering financial details.
 5. Take help from elders when necessary.
-

G. HACKING

14. What is hacking?

Answer:

Hacking is an act of gaining access to a victim's computer for the purpose of stealing information.

How can we avoid becoming a victim of hacking?

1. Use strong passwords.
 2. Change passwords frequently.
 3. Keep computers up to date.
 4. Do not connect untrusted USB drives or storage devices.
 5. Do not connect to unprotected public networks.
 6. Download apps only from trusted sources.
-

H. SPAMMING

15. What is spamming?

Answer:

Spamming refers to unwanted mails received from various unwanted sources. Most of these are advertisements. Spam can fill the inbox and prevent important mails from being noticed.

How can spam be avoided?

1. Do not give your e-mail or contact information to unnecessary websites.
 2. Do not reply to spam mails because replying may result in more unwanted mails.
-

I. VIOLATION OF PRIVACY

16. What is privacy?

Answer:

Privacy means that every person has the freedom to hide and distribute their personal information according to their choice.

How can we protect our privacy?

1. Never give out personal information unnecessarily.
 2. Use two-step authentication for e-mails.
 3. Never share credit-card details with anyone.
 4. Prefer to use cash while shopping online.
-

J. SOFTWARE PIRACY

17. What is software piracy?

Answer:

Software piracy refers to the illegal copying, distributing, sharing, selling or use of software.

Give examples of software piracy.

1. Buying software for one computer and using it on multiple computers.
 2. Installing software from unauthorised sources.
 3. Sharing downloaded software with friends and family without the creator's permission.
-

18. How can software piracy be prevented?

Answer:

1. Purchase software from authorised websites or dealers.
 2. Do not buy unauthorised software.
 3. Register software after downloading or purchasing it.
-

K. INTELLECTUAL PROPERTY RIGHTS

19. What are Intellectual Property Rights?

Answer:

Intellectual Property Rights are the rights given to an original inventor or creator to protect their invention or creation for a certain period. These rights allow the creator to have control over their creation.

20. What is copyright infringement?

Answer:

Copyright infringement occurs when someone uses, reproduces, distributes, performs or publicly displays copyrighted work without the permission of the copyright owner or without a valid licence.

21. How can Intellectual Property Rights be protected?

Answer:

1. Do not share business ideas unnecessarily.
 2. Keep detailed explanations, artwork, plans and records as proof.
 3. Register new ideas or business plans as trademarks where appropriate.
-

L. CYBERSECURITY

22. What is cybersecurity?

Answer:

Taking measures to keep yourself safe while using the Internet is known as **cybersecurity** or **cyber safety**.

23. Write the guidelines for staying safe while using the Internet.

Answer:

1. Keep antivirus software updated.
 2. Use strong passwords that are difficult to guess.
 3. Do not open suspicious e-mails or links.
 4. Never share personal details with strangers.
 5. Avoid interacting with strangers on social media.
 6. Keep privacy settings enabled.
 7. Be careful about downloads because they may contain malware.
 8. Do not post personal information on social media.
-

M. FIREWALLS

24. What is a firewall?

Answer:

A firewall is a network security measure that monitors and controls the network traffic of a computer according to a set of rules. It acts like a wall between a computer/network and potentially unwanted traffic.

25. What is the main purpose of a firewall?

Answer:

The main purpose of a firewall is to keep a network safe, regulate access to data, prevent unauthorised access and allow safe traffic while blocking malicious or unwanted traffic.

26. What are the types of firewalls mentioned in the chapter?

Answer:

The chapter describes:

1. **Software-based firewall** – protects the computer on which it is installed.
2. **Hardware-based firewall** – can protect an entire network.

The chapter also shows the evolution of firewalls from packet filtering to proxy, next-generation, cloud-based, software-defined/virtual firewalls and present-day AI/ML-related developments.

N. PARENTAL ASSISTANCE

27. What is the role of parents in keeping children safe on the Internet?

Answer:

Parents should keep an eye on their children's Internet usage and help them use the Internet safely.

They should:

1. Teach children not to accept friend requests from strangers.
2. Ask them to use authentic and secure websites.
3. Teach them how to create strong passwords.
4. Explain why passwords should not be shared.
5. Use appropriate firewall/filtering systems.
6. Encourage children to change passwords regularly.

O. DIGITAL FOOTPRINTS

28. What is a digital footprint?

Answer:

A digital footprint is an impression that a user leaves while using the Internet. It is the collection of data and information that an individual leaves through activities on digital devices and online platforms.

It is also known as a **digital dossier**.

29. How will you manage your digital footprint?

Answer:

1. Manage browser settings and control or block cookies and tracking scripts.
2. Clear browser history and cookies regularly.
3. Keep the operating system, applications and antivirus software updated.
4. Think carefully before posting personal information, photos or updates.
5. Use strong and unique passwords.
6. Enable two-factor authentication whenever possible.
7. Review privacy settings regularly.
8. Limit the personal information visible to the public.
9. Use a pseudonym or different name for some online activities where appropriate.
