JS2 - CYBERSECURITY AWARENESS

Meaning of Cybersecurity

Cybersecurity is the protection of computers, mobile phones, networks, and information from criminals, damage, theft or unauthorized access through the internet or other digital systems.
In simple words, cybersecurity means keeping our computers, phones and information safe from people who want to harm us online.

Examples of things we protect through cybersecurity:

1. Personal information.
2. Passwords.
3. Photographs and videos.
4. Bank details.
5. School records.
6. Computer files.

Importance of Cybersecurity

1. It protects our personal information.
2. It prevents hackers from accessing our accounts.
3. It protects computers from viruses.
4. It helps prevent online fraud.
5. It keeps our information safe.
6. It helps us use the internet safely.

Types of Cyberattacks

A cyberattack is an attempt by a person or group to damage, steal, or gain unauthorized access to a computer, network or personal information.
The following are common types of cyberattacks:

Virus Attack: A computer virus is a harmful program that enters a computer and can damage files or affect how the computer works. Example: Downloading an infected file that damages computer documents.

Phishing Attack: Phishing is a trick used by criminals to steal personal information such as passwords and bank details by pretending to be trusted people or organisations.
Example: Receiving a fake email claiming that your bank account will be blocked unless you click a link and enter your password.

Hacking: Hacking is gaining access to a computer, phone or online account without the owner's permission.
Example: Someone entering another person's social media account without permission.

Malware Attack

Malware is harmful software designed to damage computers, steal information or disturb normal computer activities.
Examples of malware include:

- Viruses
- Spyware
- Ransomware
- Worms

Ransomware Attack

Ransomware is a type of harmful software that locks or encrypts computer files and demands money before allowing the owner to access them again.
Example: A criminal locks a school's computer files and demands money to unlock them.

6. Password Attack

This happens when criminals try to discover or steal someone's password to gain access to their accounts.
Example: Someone guessing a student's password to enter their email account.

7. Identity Theft

Identity theft happens when someone steals another person's personal information and uses it to pretend to be that person.
Example: Someone using another person's name and photograph to create a fake social media account.

3. Safe Online Habits

Safe online habits are good behaviours we practise when using the internet to protect ourselves and our information.

The following are important safe online habits:

1. Use Strong Passwords: Create passwords that are difficult for other people to guess. Use a mixture of letters, numbers and symbols.
2. Keep Personal Information Private: Do not share your home address, phone number, passwords or private details with strangers online.
3. Avoid Suspicious Links: Do not click on strange links sent by unknown people through emails, messages or social media.
4. Install Antivirus Software: Use trusted antivirus software to help protect your computer against viruses and other harmful programs.
5. Update Your Software: Always update your computer, phone and applications to improve security.
6. Be Careful with Public Wi-Fi: Avoid entering passwords or sensitive information when using unsecured public Wi-Fi.
7. Report Suspicious Activities: Tell a parent, teacher or trusted adult if someone threatens, bullies or behaves suspiciously towards you online.
8. Use Two-Factor Authentication: Add another layer of security to your accounts, such as a verification code, where available.

4. Rules for Staying Safe on the Internet

Students should always remember these rules:

1. Never give your password to strangers.
2. Do not meet someone you know only from the internet without permission from a trusted adult.
3. Do not download files from unknown websites.
4. Do not respond to messages from suspicious people.
5. Always log out of your account when using a public computer.
6. Do not post embarrassing or private pictures online.
7. Treat other internet users with respect.
8. Tell your teacher or parents when something online makes you uncomfortable.

5. Difference Between Cybersecurity and Cyberattack

Cybersecurity	Cyberattack
It means protecting computers and information.	It means trying to harm or access computers without permission.
It helps keep users safe.	It threatens users' safety.
Example: Using antivirus software.	Example: Sending a computer virus.

Evaluation Questions

Answer the following questions in your exercise books.

1. What is cybersecurity?
2. Explain the meaning of a cyberattack.
3. Mention five types of cyberattacks.
4. What is phishing?
5. Explain the meaning of hacking.