→Dangers of using unprotected information systems:

1.Intrusion or Hacking---gaining access to a computer system without the knowledge of its owner

2. Viruses and Worms--- programs that make computer systems not to work properly

3. Trojan Horse--- These programs are having two components; one runs as a server and another one runs as a client to attack data integrity, steal private information on the target system, store key strokes and make it viewable for hackers, sending private local as an email attachment.
4. Spoofing---fooling other computer users to think that the source of their information is coming from a legitimate user
5. Sniffing---used by hackers for scanning login_ids and passwords over the wires.

6. Denial of Service---The main aim of this attack is to bring down the targeted network and make it to deny the service for legitimate users.

→Benefits of Parental Controls on devices:

1. Filter and block content that you don't want your children to see, such as violence and pornography.

2. Restrict what information is shared.

3. Set time limits on how long children are online.

4. Control the time of day that children can access the internet.

5. Set different profiles so that each family member has an access level that is appropriate to them.

→Risks of Security Violation:

1. Business disruption

2. Financial losses

3. Loss of privacy

4. Damage to reputation

5. Loss of confidence

6. Legal penalties

7. Impaired growth

8. Loss of life

→Technical means exist to restrict accesses to some services from your devices. It is possible to get them from your devices or by talking to an agent on one of our various channels.

→It is prohibited to use electronic communication networks for the publishing of illicit content or any other act that is likely to affect the security of networks or information systems.

→It is prohibited to design misleading viruses, spywares, potentially undesirable software or any other device leading to fraudulent practices.