**Nguyễn Công Cường - 20T1**

**UNIT 5**

**Task 1**

1. The jump instruction alters the normal execution sequence, allowing the virus to run first.
2. Main parts: misdirection, reproduction, trigger, payload.
3. The last act is the payload routine, which can be harmful.

**Task 2**

* The virus replaces the first instruction with a jump command to run its code first.

**Task 3**

1. Computer viruses are like biological viruses as they infect and reproduce using the host's resources.
2. Patching enables the virus to detect files like COM or EXE and copy itself.
3. Some viruses stay in memory to continue infecting other programs.
4. Payload examples: showing messages, deleting files.
5. Viruses often attach to COM and EXE files.
   * 1-c
   * 2-b
   * 3-d
   * 4-a
6. A Trojan lacks a reproduction routine.

**Task 4**

1. Logic bomb: Destroys payroll records.
2. Form: Corrupts floppies, triggers key beeps.
3. Beijing: Displays message.
4. AntiEXE: Overwrites disk, causing data loss.
5. Cascade: Makes text characters fall on the screen.
6. Macro virus: Attaches to documents and spreads, causing various harms.

**Task 5**

1. Encodes
2. Encourages
3. Enhanced
4. Enables
5. Encrypt
6. Ensure
7. Brighten
8. Enlarge
9. Enable
10. Widen

**Task 6**

1. b
2. h
3. c
4. a
5. e
6. g
7. f
8. d
9. j
10. i

**Task 7**

1. Use antivirus software.
2. Use strong, unique passwords.
3. Regular backups.
4. Lock the lab and use physical security measures.
5. Test backup tapes regularly.

**Task 8**

* Antivirus software
* Strong passwords
* Backup systems
* Locking devices
* UPS to prevent power loss

**Task 9**

1. Backup copies
2. Shareware
3. Tamperproof
4. Compromise
5. Decoded
6. Encrypt
7. Firewall
8. Monitor
9. Biometric
10. Regularly

**Task 10**

* + a → b → c → d → e → f
  + a → b → c → d → e
  + f → g
  + a → b → c → d → e → g
  + f → h

**Task 11**

1. Firewall
2. Erase
3. Trigger
4. Detect
5. Initiate
6. Carrier
7. Pirated
8. Boot

**Task 12**

1. Serious, it caused a lot of damage.
2. b. About right.
3. Yes, other hacking incidents exist, e.g., ransomware attacks.