Grade 12 A/L ICT · Lesson 6

6.11 Network Security: Threats and Protection

Syllabus 6.11. The open Internet lacks built-in confidentiality. **Public/private keys** support **encryption** and **digital signatures**. You list **threats** (viruses, Trojans, malware, phishing) and **protection** (firewalls, antivirus, awareness).

1. Confidentiality and keys

Encryption hides content; **digital signatures** help authenticate the sender. **Public** key encrypts / verifies; matching **private** key decrypts / signs (basic idea).

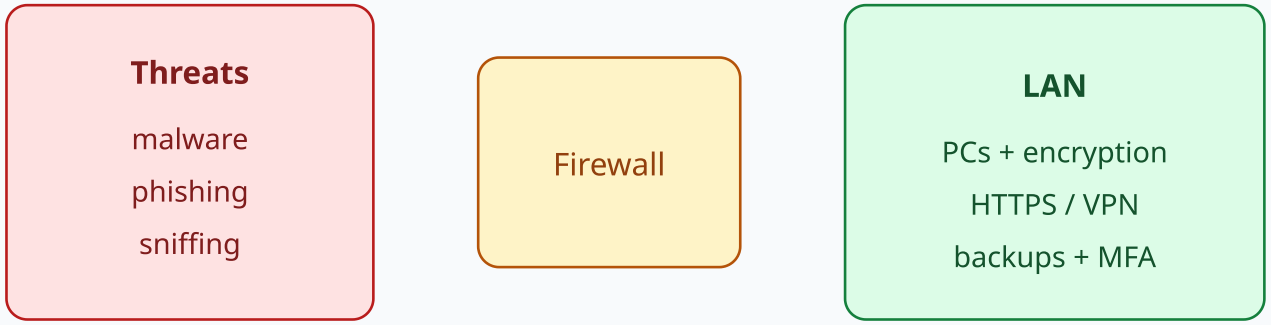
2. Threats

- **Virus** – spreads by infecting files/programs.
- **Trojan** – looks useful, hides harm.
- **Malware** – broad term for bad software.
- **Phishing** – tricks people into giving secrets.

3. Protection

Firewalls filter traffic; **antivirus** detects malware; **education** and good passwords/updates stop many attacks.

Threats, firewall and protected LAN



Firewall between threats and LAN

🧱 **Worked example: Phishing link to a fake bank. Defence: check URL, use HTTPS, MFA, never email passwords.**
Firewall + encryption + user caution reduce risk.

© 2026 schoolict.net (Ruwan Mangala Suraweera) · All rights reserved

🚀 **Beyond the syllabus (2026 update)** *Not required for the exam – read for interest.* Passkeys and zero-trust are modern trends; syllabus wants keys, threats and basic defences.

Key Words

Encryption – Scrambling data for confidentiality.	**Digital signature** – Proves origin/integrity with keys.
Public key – Shared key for encrypt/verify.	**Private key** – Secret key for decrypt/sign.
Virus – Self-spreading infection of programs.	**Trojan** – Malware disguised as useful software.
Malware – Malicious software (general).	**Phishing** – Social engineering for secrets.
Firewall – Filters network traffic.	**Antivirus** – Detects/removes malware.
Authentication – Confirming identity.	**Confidentiality** – Keeping data private.

Sample Q&A

1. Why encrypt?

> **Answer:** Confidentiality on an open network.

2. Public vs private key (one line).

> **Answer:** Public shared; private kept secret.

3. Phishing?

> **Answer:** Tricking users into revealing secrets.

4. Firewall role?

> **Answer:** Filter allowed/denied traffic.

5. Trojan vs virus (brief).

> **Answer:** Trojan disguises; virus spreads by infection.

6. Name three protections.

> **Answer:** Firewall, antivirus, user awareness.

© 2026 schoolict.net (Ruwan Mangala Suraweera) · All rights reserved

MCQ

1. Encryption mainly provides

A. confidentiality
B. chair height
C. mouse DPI
D. font size
E. cable colour

2. A private key should be

A. emailed to strangers
B. printed on buses
C. painted on walls
D. kept secret
E. posted publicly

3. Phishing attacks

A. only hub LEDs
B. trick people
C. only fan noise
D. only fiber photons
E. only copper atoms

4. A firewall

A. irons shirts
B. draws cartoons
C. filters network traffic
D. boils water
E. cuts paper

5. Malware means

A. marble statues
B. malicious software
C. maths homework
D. milk cartons
E. musical software only

6. Digital signatures help with

A. folding chairs
B. warming GPUs
C. painting MAC
D. making tea
E. authentication / integrity

© 2026 schoolict.net (Ruwan Mangala Suraweera) · All rights reserved

7. Antivirus software

A. brews coffee
B. detects malware
C. builds buses
D. tunes guitars
E. assigns IPv6 only

8. The open Internet alone does not guarantee

A. confidentiality and authentication
B. that chairs have legs
C. that light travels
D. that paper is dry
E. that copper exists

9. Which term means: “Scrambling data for confidentiality”?

A. Public key
B. Phishing
C. Encryption
D. Authentication
E. Trojan

10. Which term means: “Proves origin/integrity with keys”?

A. Digital signature
B. Malware
C. Private key
D. Confidentiality
E. Firewall

11. Which term means: “Shared key for encrypt/verify”?

A. Encryption
B. Virus
C. Antivirus
D. Phishing
E. Public key

12. Which term means: “Secret key for decrypt/sign”?

A. Digital signature
B. Firewall
C. Trojan
D. Private key
E. Authentication

© 2026 schoolict.net (Ruwan Mangala Suraweera) · All rights reserved

13. Which term means: “Self-spreading infection of programs”?

A. Antivirus
B. Confidentiality
C. Public key
D. Malware
E. Virus

14. Which term means: “Malware disguised as useful software”?

A. Private key
B. Phishing
C. Authentication
D. Trojan
E. Encryption

15. Which term means: “Malicious software (general)”?

A. Virus
B. Firewall
C. Confidentiality
D. Malware
E. Digital signature

16. Which term means: “Social engineering for secrets”?

A. Phishing
B. Antivirus
C. Public key
D. Encryption
E. Trojan

17. Which term means: “Filters network traffic”?

A. Malware
B. Firewall
C. Authentication
D. Private key
E. Digital signature

18. Which term means: “Detects/removes malware”?

A. Confidentiality
B. Virus
C. Public key
D. Phishing
E. Antivirus

© 2026 schoolict.net (Ruwan Mangala Suraweera) · All rights reserved

19. Which term means: “Confirming identity”?

A. Firewall
B. Trojan
C. Authentication
D. Private key
E. Encryption

20. Which term means: “Keeping data private”?

A. Antivirus
B. Digital signature
C. Confidentiality
D. Virus
E. Malware

Structured Questions

1. Need for confidentiality and authentication. *(2 marks)*

> Internet does not provide them by default.

2. Public/private keys for encrypt and sign. *(2 marks)*

> Public encrypt/verify; private decrypt/sign.

3. Four threats with one line each. *(4 marks)*

> Virus; Trojan; malware; phishing.

4. Three protections. *(3 marks)*

> Firewall; antivirus; awareness/practices.

5. One school-lab safe practice. *(2 marks)*

> Strong passwords / do not open unknown links.

Summary

- Keys enable secrecy and signatures.
- Threats: virus, Trojan, malware, phishing.
- Firewalls filter traffic.
- Antivirus + updates.
- Awareness stops many attacks.

© 2026 schoolict.net (Ruwan Mangala Suraweera) · All rights reserved

MCQ answer key – 6.11

1. **A** – Privacy of content.
2. **D** – Secret.
3. **B** – People.
4. **C** – Filters.
5. **B** – Bad software.
6. **E** – Auth/integrity.
7. **B** – Detect malware.
8. **A** – No built-in secrecy.
9. **C** – Encryption – Scrambling data for confidentiality.
10. **A** – Digital signature – Proves origin/integrity with keys.
11. **E** – Public key – Shared key for encrypt/verify.
12. **D** – Private key – Secret key for decrypt/sign.
13. **E** – Virus – Self-spreading infection of programs.
14. **D** – Trojan – Malware disguised as useful software.
15. **D** – Malware – Malicious software (general).
16. **A** – Phishing – Social engineering for secrets.
17. **B** – Firewall – Filters network traffic.
18. **E** – Antivirus – Detects/removes malware.
19. **C** – Authentication – Confirming identity.
20. **C** – Confidentiality – Keeping data private.

© 2026 schoolict.net (Ruwan Mangala Suraweera). All rights reserved.