

PART TWO

Information Technology Technical Question

3 mins

In this part of the exam, you will talk about **Security Risks on the Internet (phishing, malware, spam...)**. The following ideas will help you.

- What are some security risks on the internet.
- Explain what Phishing, Malware, Spam, Viruses and Social Engineering are.
- What steps can you take to protect yourself online?

2A



2B



PART TWO

Information Technology Technical Question

3 mins

In this part of the exam, you will talk about Security Risks on the Internet (phishing, malware, spam...). The following ideas will help you.

- What are some security risks on the internet.
- Explain what Phishing, Malware, Spam, Viruses and Social Engineering are.
 - **Phishing:** This involves fraudulent attempts to obtain sensitive information by disguising communications as coming from trustworthy sources. Phishing schemes often exploit email, phone calls, or text messages to lure victims into sharing confidential information or clicking on malicious links.
 - **Malware:** Malware includes viruses, worms, spyware, and ransomware. It is designed to infiltrate and damage systems. Ransomware, a type of malware, holds data or systems captive until a ransom is paid.
 - **Spam:** Unsolicited messages, often sent in bulk, can clutter your inbox and sometimes contain malicious links or attachments. Spam can also be used in phishing attacks to trick users into revealing personal information.
 - **Viruses:** These are hostile programs that attach themselves to legitimate files and spread to other files and systems, causing damage and disruption.
 - **Social Engineering:** This involves manipulating individuals into divulging confidential information. Attackers often exploit human psychology rather than technical vulnerabilities
- What steps can you take to protect yourself online?
Use strong, unique passwords, be cautious of unsolicited communications, keep your software updated, and use reliable security software.



2A



2B