

Cambridge Advanced National (AAQ) in IT in Cyber Security and Networks

The key features of Cambridge Advanced Nationals (AAQ) in Cyber Security and Networks is to:

- Develop key knowledge, understanding and skills relating to the fundamentals of cyber security.
- Think creatively, innovatively, analytically, logically and critically
- Develop valuable communication skills that are important in all aspects of further study and life

Fundamentals of Cyber Security (Exam)

In this unit you will learn why cyber security is important to us all and the motivations of different threat actors. You will learn what cyber security threats look like, how threats function and the steps that can be taken by individuals and organisations to protect, detect and respond to them. Topics include:

- Topic Area 1 The cyber security landscape
- Topic Area 2 Cyber security vulnerabilities
- Topic Area 3 Impact of cyber security events
- Topic Area 4 Cyber security mitigations
- Topic Area 5 Policies, procedures, and event handling
- Topic Area 6 Job roles and responsibilities

Preventing Cyberattacks (NEA)

In this unit you will learn techniques to assess for risks to networks, devices and applications and produce risk assessments. You will learn how to audit the measures used to prevent cyberattacks, design policies that control access to systems and educate users in cyberattack prevention. Topics include:

- Topic Area 1 Cyber Security Aims and Threats
- Topic Area 2 Identify risks to networks and data
- Topic Area 3 Audit and improve cyberattack prevention measures
- Topic Area 4 Design access controls policies
- Topic Area 5 Design written user policies
- Topic Area 6 Review designed cyberattack prevention measures

Fundamentals of Networks (Exam)

In this unit you will learn about the fundamental concepts of networks, including different models, addressing techniques and protocols. You will also learn about the different hardware devices that are used in a network and how those devices are connected. Topics include

- Topic Area 1 Network types, models, topologies and services
- Topic Area 2 Network layers, protocols and addressing
- Topic Area 3 Wired network components
- Topic Area 4 Mobile and wireless networks
- Topic Area 5 Network performance
- Topic Area 6 Cloud networks

Digital forensic investigation (NEA)

In this unit you will learn about digital forensics including the processes followed when completing digital forensic investigations. You will plan digital forensic investigations and use software tools to extract evidence and present evidence ready for use in court. Topics include:

- Topic Area 1 Fundamentals of digital forensics
- Topic Area 2 Plan digital forensic investigations
- Topic Area 3 Collect, preserve and analyse digital evidence
- Topic Area 4 Report digital forensic investigation findings
- Topic Area 5 Review digital forensic investigations

Penetration testing and incident response (NEA)

In this unit you will learn about penetration testing strategies and plan penetration tests. You will learn how to undertake planned exploits on vulnerable systems, using specific methods and tools. You will create cyber security incident response plans, incident playbooks and maintenance plans to build and upkeep incident response capability. Topics include:

- Topic Area 1 Introduction to penetration testing
- Topic Area 2 Plan penetration testing
- Topic Area 3 Implement penetration testing scoping plans
- Topic Area 4 Incident response planning
- Topic Area 5 Develop cyber security incident response capability
- Topic Area 6 Review penetration testing and incident response capability

Other Optional Units include:

- **F198: Implementing secure local area networks (LANs) (NEA)**
- **F199: Designing and communicating secure global computing systems (NEA)**

Work you can do to prepare for A Level

During the course we will use examples of the leading Computer Hardware, Software (including AI large language learning models) as well as Networking Companies such as Palantir, Nvidia, Microsoft, Cisco, Meta, Google, Amazon, Apple and many more!

It is recommended you research the big names and consider advancements in AI, large language learning models/neural networks as well as ChatGTP. Consider how Nvidia GPU semiconductors are driving the market. Consider how autonomous technology and robotics are set to impact on and change what we do. How Google and IBM are leading the way with Quantum Computing carrying out complex computations in minutes that would take classical supercomputers 10 septillion years to complete!

- **Palantir** – Alex Karp
- **NVidia** – Jenson Huang
- **Google** – Sundar Pichai
- **Apple** – Tim Cook
- **Meta** – Mark Zuckerberg

The types of courses you may progress to Both the subject-specific knowledge, understanding and skills, and broader transferable skills developed in this qualification will help you progress to further study in related areas such as:

- BSc (hons) Computer Networks and Cyber Security
- BSc (hons) Computer Science with Cyber Security
- BSc (hons) Cyber Security
- BSc (hons) Cyber Security and Digital Forensics
- BSc (hons) Cyber Security Management.

Resource links:

- A Level IT AAQ revision guide
- Educa8 – <https://educa8.co.uk>
- Use www.youtube.com videos on topics you find difficult
- Use your Y12 & 13 'Very Important Notes' (VINs) for revision
- Use <https://quizlet.com/login> to test yourself on content
- Use <https://create.kahoot.it/login> to test yourself on content
- Revise the meanings of the keywords in the specification

Entry Requirements:

You will ideally have studied IT or Computing Science at GCSE level (but not essential) but you will have an interest in IT or Computing; have a minimum of Grade 4 in English and Maths.

Specification:

<https://www.ocr.org.uk/Images/733888-specification-cambridge-advanced-nationals-cyber-security-and-networks.pdf?hsCtaAttrib=189589178278>