The BSc (Hons) Cyber Security Technical Professional Degree Apprenticeship is designed to enhance and accelerate cyber skills. It is a work-based learning programme that develops advanced understanding of cyber security issues and technology solutions.

It is a structured, research-rich learning programme that includes a range of learning experiences – including classroom workshops and work-based activities. As a work-based programme, it supports development of skills needed within an organisational context.

Students will develop, update, extend and deepen their knowledge and technical competency. Combined with enhancing professional skills and behaviours, it empowers students to excel in the field of cyber security.

DURATION: 4 years
AWARD: BSc (Hons) Cyber Security Technical Professional, awarded by Northumbria University, Newcastle
APPRENTICESHIP STANDARD: Cyber Security Technical Professional (Integrated Degree)
ENTRY REQUIREMENTS: 120 UCAS tariff points

This apprenticeship is delivered in partnership with Northumbria University, Newcastle

MODE OF STUDY: Part-Time, blended and work-based learning
ASSESSMENT METHODS: Coursework including portfolios and the End Point Assessment (EPA)
START DATE(S): October, January, April, July
LOCATIONS: London, Birmingham, Manchester, Newcastle, Bristol
SECURITY STARTS WITH CYBER SKILLS

This degree apprenticeship equips people to work in a range of computing, IT, and digital technology roles where cyber security plays a vital role. This programme uses a range of different ways to learn.

Work-based activities, digital learning and online resources develop students' knowledge throughout the programme. Students also attend face-to-face workshops at a local QA training centre to help contextualise learning. 20% of working time is required for studying – we will talk you through this.

This learner journey gives you an overview of the programme.

LEVEL 4
- Computer Systems and Digital Logic (Core)
- Algorithms and Mathematics (Core)
- Software Development (Core)
- Operating Systems and Server Administration (Core)
- Human Computer Interaction and Cyber Security (Core)
- Professional Practice 1 (Core)

Each module has 2x 2-day block workshops (6 hours per day)

LEVEL 5
- Computer Security (Core)
- Web and Mobile Application Security (Core)
- Network Security (Core)
- Data Science and Cyber Security (Core)
- Ethical Hacking (Core)
- Professional Practice 2 (Core)

Each module has 3x 2-day and 1 x 1-day block workshop (6 hours per day)

LEVEL 6
- Digital Forensics and Incident Handling (Core)
- Information Security Management (Core)
- Cyber Offensive Defence (Core)
- Cyber Security Project (Core, 30 credits)
- Professional Practice 3 (Core)
- Cyber Security Technical Professional End Point Assessment (EPA) (Core, 10 credits)

Each module has 2x 1-day workshops (6 hours per day)

What is Professional Practice?
These are self-guided modules that allow students to tailor the programme to the environment they work in. They are an opportunity to develop specialist cyber security skills.

Before completing their EPA, students must have:
- passed all the other modules in this programme
- agreement from their employer that they are ready for the EPA
- completed the e-portfolio
- completed level 2 English and maths qualifications (if not already achieved)

Full details of the EPA can be found online.