OpenLearn

The Open University

Statement of participation

Jesse Bruce

has completed the free course including any mandatory tests for:

Network security

This 25hour free course discussed network security and the intricacies of maintaining system resilience. It assumed an advanced knowledge of computing

Issue date: 1 August 2017

www.open.edu/openlearn

This statement does not imply the award of credit points nor the conferment of a University Qualification.
This statement confirms that this free course and all mandatory tests were passed by the learner.
Please go to the course on OpenLearn for full details:
http://www.open.edu/openlearn/science-maths-technology/computing-and-ict/systems-computer/network-security/content-section-0

COURSE CODE: T823_1

OpenLearn

The Open University

Network security

http://www.open.edu/openlearn/science-maths-technology/computing-and-ict/systems-computer/network-security/content-section-0

Course summary

Encryption of files and firewalls are just some of the security measures that can be used in security. This free course, Network security, which assumes you have a substantial knowledge of computing, helps to explain the intricacies of the continually changing area of network security by studying the main issues involved in achieving a reasonable degree of resilience against attacks.

Learning outcomes

By completing this course, the learner should be able to:

- identify some of the factors driving the need for network security
- identify and classify particular examples of attacks
- define the terms vulnerability, threat and attack
- identify physical points of vulnerability in simple networks
- compare and contrast symmetric and asymmetric encryption systems and their vulnerability to attack, and explain the characteristics of hybrid systems.

Completed study

The learner has completed the following:

Section 1

Terminology and abbreviations

Section 2

Background to network security

Section 3

Threats to communication networks

Section 4

Principles of encryption

Section 5

Implementing encryption in networks

Section 6

Integrity

Section 7

Freshness

Section 8

Authentication

Section 9

Access control

Section 10

Conclusion