

BTEC Assignment Brief

Qualification	Pearson BTEC Level 3 National Diploma in Computing
Unit number and title	Unit 7: IT Systems Security and Encryption
Learning aim(s) (For NQF only)	<p>C: Examine the techniques used to protect an IT system from security threats</p> <p>D: Implement strategies to protect an IT system from security threats</p>
Assignment title	IT security threats and cryptography
Assessor	C Johnston
Issue date	09-05-2018
Hand in deadline	08-06-2018

Vocational Scenario or Context	<p>You work for a start-up company who are developing internet based financial transfer software which allows people to transfer money quickly and cheaply to friends and family both at home and abroad. Following on from your report on current security threats you have been asked to carry out an investigation into the protection methods than can be used and to apply these to a 'guinea-pig' system to check they work as expected.</p>
---------------------------------------	--

Task 1	<p>Plan, implement and review protection techniques</p> <p>Write a report for the company directors in which you explain the physical, organisational and software techniques which should be used to protect their systems from security threats.</p> <p>Set up a computer system in which you plan and apply appropriate security protection methods. The system you set up needs to:</p> <ul style="list-style-type: none"> • support different groups of users. This will allow you to show how to you can control the access users have to each other's files • connect to a Wi-Fi network so you can demonstrate how to set up the security for this type of network • connect to the internet so you can show how to set up a Firewall to protect the system and restrict access to it • have anti-virus software installed and configured. <p>You need to create a portfolio of evidence including:</p>
---------------	--

	<ul style="list-style-type: none"> • a plan and justification of the physical and software protection measures that you will apply to the system • the implementation of the security measures you have planned (e.g. screen shots of the installation and configuration of protection methods) • a test plan showing the testing of the security measures you have applied to confirm they work as intended • a review of the extent to which the system has been protected from security threats • based on the testing and review of the protection applied, enhancements to the protection, for example by minimising the impact of the protection methods on the performance and usability of the system • an evaluation of both the plan you created, the implementation of the plan and the overall effectiveness of the measures you have applied. <p>You also need to provide evidence that you have shown individual responsibility and effective time management in the planning and implementation of the protection applied to the server.</p>
Checklist of evidence required	<p>Report on the protection methods which should be used. Annotated photographic/video evidence of protection measures applied to an IT system. Completed test plan, including reviews of the protected IT system. Annotated photographic/video evidence of improvements and optimisations being made to an IT system. Written or audio/video recorded justification of planning decisions and an evaluation of the plan and the protected IT system. Evidence of individual responsibility and effective time management such as notes, diary entries, witness testimonies, discussion notes or recordings</p>
Criteria covered by this task:	
Unit/Criteria reference	To achieve the criteria you must show that you are able to:
7/CD.D2	Evaluate the plan and the effectiveness of the protected IT system against requirements.
7/CD.D3	Demonstrate individual responsibility and effective self-management in the planning and protection of an IT system.
7/C.M3	Justify the choice of protection techniques used to defend the IT systems of an organisation, showing how its IT system will be protected from security threats.
7/D.M4	Enhance the protection of the IT system which to meet requirements given in the plan.
7/C.P5	Explain how protection techniques can help defend an organisation from security threats.
7/C.P6	Produce a plan to protect an IT system which meets organisational and

	legislative requirements.
7/D.P7	Perform tasks to protect the IT system which meets the requirements given in the plan.
7/D.P8	Review the extent to which the organisation's IT system has been 'protected'.
Sources of information to support you with this Assignment	<ul style="list-style-type: none"> • BBC News Technology section – technology news, including cases of significant cyber-attacks: www.bbc.co.uk/news/technology • McAfee's security advice centre – provides useful and up-to-date information on security, virus attacks and viruses, written in a reasonably accessible manner: home.mcafee.com/advicecenter/ • Microsoft's security advice centre – features a regularly updated blog and FAQ on security issues: www.microsoft.com/security/ • Norton's security centre – provides articles on security, spam email, software piracy, etc.: uk.norton.com/security-center/
Other assessment materials attached to this Assignment Brief	<i>eg, work sheets, risk assessments, case study</i>