UNIT 7: IT SYSTEMS SECURITY AND ENCRYPTION

Delivery guidance

Approaching the unit

IT security is one of the primary issues for IT professionals, so this unit is of critical importance to all computing learners. It is a highly dynamic area of the industry, as technological developments are constantly happening, in addition to newly discovered security threats. In many ways, IT security is a struggle between cybercriminals and computing professionals trying to protect personal and business IT systems. While this is an exciting and fascinating topic of study for learners to engage with, it can also prove challenging to keep up to date with the latest developments, and you will need to carry out regular research.

This delivery guide does not cover everything that needs to be delivered for completion of this unit but gives examples of delivery methods. You should refer to the specification for full details of all the content that needs to be covered.

Delivering the learning aims

For learning aim A, you could start with a class discussion about security issues. Many learners will have some experience of this topic and are likely to have heard of some well-known security breaches. However, much of their knowledge is likely to relate to their personal IT use, and you should make it clear that this issue is also of vital importance to business users. It might be useful to set learners some research tasks, asking them to look into the most recent examples of data breaches, virus attacks and politically-motivated hacking.

Topic A4 concerns legal requirements, so, to engage your learners, you could ask them to research people, companies or organisations who have broken these laws, covering not only what they did but also the laws that they broke and the eventual outcome.

Cryptography, covered in learning aim B is an interesting but largely theoretical topic that can be very complex. Its history pre-dates the computing age and, of course, code cracking was one of the first purposes that computers were used for. It is worth reminding learners that this technology underpins the internet age and without it there would be no e-commerce, online banking etc. Learning aim B offers many opportunities to engage and enthuse learners, as code cracking is a subject that most of them will find interesting and challenging.

Learning aim C concerns the techniques used to protect IT systems, and so is linked with the threats covered in learning aim A. You could link the two learning aims together, covering the threat and then the associated protection methods. Another possible approach would be to build on the research task of looking at recent examples of data breaches, virus attacks etc, and ask learners to consider what protection methods might have been effective in preventing the problems they have researched.

You could enliven topic C2, covering policies and procedures, by looking at several different IT, internet or network usage policies, perhaps taking your own centre’s policies and comparing them with policies from different types of organisation. You could focus on the purpose of each part of the policies and discuss their appropriateness.

You could also consider delivering topic C3 in conjunction with the associated practical tasks in topic D. This will help to ensure that learners can see clearly that the theoretical content relating to software-based protection links to the practical applications.

For learning aim D, learners will need access to systems on which they can practise their skills. It is highly unlikely that they will be allowed to adjust the security settings on the live computing systems within your school or college, so you have two options. You could:

- have separate, dedicated, unrestricted computer systems which are not directly connected to the main college/school system
- use virtual PCs – there are a number of software products that allow you to install a software-emulated virtual PC, such as VirtualBox®.

You will also need to supply a WiFi access point for learners to set up and configure in order to cover topic D4. You can obtain these from a range of IT equipment suppliers.

Throughout their practical work, learners should be encouraged to keep a diary, in which they can record their progress, any issues they encountered and how they overcame them. This will be valuable to them when they are writing their evaluation and reflecting on their own performance as part of the second assignment.

High quality, accurate verbal and written communication skills are vital for progression into higher education and in employment. As such, learners should be confident in presenting thoughts and ideas to others, as well as producing well-presented, accurate and appropriate documentation for all stages of a project. Learners must be able to effectively evaluate the success of a project and the factors that contributed to the final outcome, including their own skills, knowledge and behaviours.

Learning aim	Key content areas	Recommended assessment approach
A Understand current IT security threats, information security and the legal requirements affecting the security of IT systems	**A1** Threat types **A2** Computer network-based threats **A3** Information security **A4** Legal requirement **A5** Impact of security breaches	A report explaining different IT security threats, their potential impact on organisations and the principles of information security, and why organisations must adhere to legal requirements when considering security. A report explaining the principles and uses of cryptography, and an assessment on the impact of encryption and security protection, in general, on security and legal issues. An evaluation of the effectiveness of different protection techniques.
B Investigate cryptographic techniques and processes used to protect data	**B1** Cryptographic principles **B2** Cryptographic methods **B3** Applications of cryptography	
C Examine the techniques used to protect an IT system from security threats	**C1** Physical security **C2** Policies and procedures **C3** Software-based protection	Detailed testing documentation explaining how protection techniques can help defend an organisation and a plan showing the protection to be applied to a system to meet specific requirements. Annotated photographic/video evidence of protection measures applied to an IT system. Completed review 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 protected IT system. A report evaluating the plan and the protected system against the requirements.
D Implement strategies to protect an IT system from security threats	**D1** Group policies **D2** Anti-malware protection **D3** Firewall configuration **D4** Wireless security **D5** Access control **D6** Testing and reviewing protection applied to an IT system **D7** Skills, knowledge and behaviours	

Assessment guidance

This is an internally assessed unit, meaning that learners need to complete assignments that are devised and marked internally and that cover the learning aims. Learning aims A and B are theoretical in nature and the assignment should be based on a case study for a real or fictitious organisation. Evidence could be in the form of a written report or a presentation (with slides and notes) to be given to the company's managers. Alternatively, you could film learners giving their presentations. A blog or some form of audio or visual evidence would also be acceptable and would allow learners to develop their creativity, provided the information is communicated in a clear and detailed manner using appropriate language.

Learning aim C requires learners to examine the techniques that can be used to protect systems, and learning aim D requires them to apply security protection to an IT system. It makes sense to combine these two learning aims into a single assignment. Supply learners with a scenario that has sufficient detail for them to meet the assessment criteria, firstly, covering the theory behind the protection techniques (for learning aim C), then implementing them (for learning aim D). For example, within the scenario, learners need requirements for different levels of access control (read, modify etc) to various folders for different users or groups, and the system should require connection to the internet and a WiFi network. The scenario should also give sufficient details of the applications and user access required to allow the learners to justify their choice of protection strategies.

The system can be a physical computer system or a virtualised environment. Learners need to put together a portfolio of evidence showing that they planned the protection strategies and can justify their choices. They need to collect evidence of applying the security measures, such as screenshots, photos, videos, witness testimony and so on, and evidence that they have refined and optimised the protection. They also need to include the test plan that they used to test the protected system and a written or audio-/video-recorded evaluation of their plan and its implementation. Learners may find it helpful to maintain a diary of their progress in setting up the system, as this could help them to evaluate the protected system.

Getting started

This gives you a starting place for one way of delivering the unit, based around the suggested assignments and tasks in the specification.

Unit 7: IT Systems Security and Encryption

Introduction

Security is a key issue in computing. The aim of this unit is to give learners a clear understanding of the threats faced by every computer system and to give them the skills to apply basic protection techniques, in order to keep a system secure.

Learning aim A – Understand current IT security threats, information security and the legal requirements affecting the security of IT systems

- You might begin by having a class discussion about learners' own experiences of security issues and cyber-attacks that have recently been in the news.
- Learners could work in small groups to research well-known or recent security issues and then present their findings back to the whole class, giving details of the attack. Try to ensure that at least one example from each type of threat is covered in topic A1 (for example, internal threats, external threats, physical threats, and social engineering and software-driven threats). Facilitate further discussion about how it might have been possible to prevent the attacks. Discuss how IT practitioners need to be proactive in terms of promoting IT security as well as being reactive and knowing what to do in the case of a security breach. You could extend the discussion by asking learners to consider the impact of these breaches, relating their responses to content covered in topic A4.
- As IT security is such a fast-moving field, it would be beneficial to ask learners to research the most recently identified threats and breaches. Learners could work in small groups to prepare a brief presentation on threats or security breaches that have occurred in the last six months. Give each group a different recent threat or type of threat to look at. Encourage them not just to look at the mechanism of the threat itself, and the details of the security breach, but also to consider the impact and possible methods of prevention. The technology section of the BBC News website could prove a useful starting point for learners' research, along with industry publications like Computer Weekly and Computing which are both available online.
- Learners need to understand that requirements for protecting home personal computers from security threats are different from those required for organisations' systems, and that the consequences of security breaches are different for individuals and organisations. It may be difficult to get industry speakers to talk about specific issues or protection methods, but it would be useful to find someone willing to talk to learners about the general security issues and consequences faced by businesses. One option is to explore the UK Cyber Security Forum website where the UK has been split into clusters. Information about member companies and regional clusters is available and you could then contact a cluster to find a potential business to work with.
- Learners could explore the topic of information security through paired work. They could consider some examples of confidential information (eg bank details and health records) and explore how the principles of confidentiality, integrity and availability apply to these. They should also discuss how the data might be misused. Finally, they should consider the impact and potential legal implications of such data being stolen or lost, both for an individual and for the company or

organisation that stored the data.

- Learners could examine legal requirements using case studies. They could investigate individuals or companies prosecuted under these laws. They can report back on what actually happened, how the legislation was applied and what the consequences were. Learners can find details on the Information Commissioner’s Office (ICO) website, which lists details of cases where they have taken action under the Data Protection Act.

Learning aim B – Investigate cryptographic techniques and processes used to protect data

- Cryptography has a very long history (that dates back to classical Greek times) and learners might find it interesting to look into the history and use of cryptography and its modern equivalents (eg steganography) and many of the features of historical cryptography that underpin the ways it is used today. Group work and research will work well with these topics. If it is possible to arrange a visit to Bletchley Park, near Milton Keynes, this will give learners a useful insight into the history of cryptography.
- You can introduce some basic cryptographic principles in an interesting and practical way by asking learners to attempt to create simple ciphers (for example using shift ciphers and one-time pads) and then attempting to crack each other’s ciphers.
- Public key encryption, as used in secure online transactions, is the most widely used modern application of cryptography, but it is quite a complex process to understand. Careful explanation will be required. A search on YouTube or other video-sharing website for ‘public key encryption’ or ‘asymmetric encryption’ will list a number of videos, many of which are clear and well explained.

Learning aim C – Examine the techniques used to protect an IT system from security threats

- You could start by looking at some of the threats that learners identified in learning aim A, and then follow this up with a discussion of the ways in which IT systems can be protected from specific threats.
- Use case studies to allow learners to investigate the physical security measures that could be applied to a specified business IT system. This is an opportunity to consider some of the areas of development such as multimodal biometric authentication systems, cloud-based biometric solutions or biometric single signs (SSO). There are other examples such as the use facial recognition to make payments (dubbed the Selfie Payment System) or using facial recognition to authenticate credit cards. Encourage learners to bear in mind the need to balance the level of threat, the usability of systems and the cost of protection. For example, ask them to consider a number of different scenarios, ranging from top-secret military data to simple business data, such as price lists, and consider what sort of protection would be appropriate in each scenario.
- You may be able to arrange a class visit from a system manager employed by a local organisation. You could ask them to talk to your learners about the backup and disaster recovery procedures that they use and their organisation’s general approach to security. However, you should remind learners that it is unlikely that the visiting speaker will be willing to talk about specific security measures that their organisation takes.
- To cover the topic of policies and procedures, learners could work in small groups to look at some given examples of internet usage policies. You could use the policies of your centre and local employers, where possible, or an internet search will produce many global examples. Ask learners to identify the reasons for the ‘dos’

and 'don'ts' given in these policies, and see if they can spot any omissions without prompting.

- It would be useful to deliver topic B3 (software protection) in combination with learning aim C. Using this approach, learners could first investigate a software-based protection technique and then attend a practical session where they practise configuring and testing the protection technique.
- This learning aim gives learners opportunities to investigate user authentication, which is an area that learners will have experienced (eg by signing into school or college systems, social media sites, banking websites or email services). In groups or as individuals, learners could research password-related issues, such as how to deal with the large number of passwords that users require for accounts on different websites (and how those websites hold those authentication details securely), password good practice, non-text-based passwords and other alternative authentication methods. Learners could also research and debate the issue of security versus usability, which they will have to consider for topic C6.
- Encryption is an interesting topic that gives plenty of scope for investigation and discussion. You could ask learners to work in small groups to create a variety of simple cyphers, perhaps with a spreadsheet. Ask them to send messages to each other using their cyphers, while the other groups attempt to crack the codes and decipher the messages. This activity could then lead into a discussion about the difficulties involved in creating cyphers and giving cyphers to the receiver in order to allow them to decode the message.

Learning aim D – Implement strategies to protect an IT system from security threats

- This learning aim is primarily practical, with learners practising how to implement the various protection methods that they have examined in learning aim B. They could do this on a physical IT system that is separate from the school or college's live systems or alternatively, if this is not possible, they could do it on a virtualised environment.
- Give learners a case study that explains the system that they are helping to set up and the levels of access they need to give to different users. Working in pairs, learners could then set up the required folder access controls and test that their set-up works correctly and gives the correct levels of access.
- When it comes to setting up anti-malware software, firewalls and wireless network security, the results are likely to be predicable if all the learners follow the same procedures. It could be more interesting to ask learners to work in groups and configure these items differently, and then compare the results in a whole class discussion. If network restrictions make it difficult to try out different settings to see how they affect different applications, you could set this as a homework task for learners to try out on their home computers and ask them to report back to the rest of the class on their findings. However, you will need to remind learners not to switch off these features or configure them in a way that would compromise the security of their home systems.
- Learners often struggle to test and review their own work effectively, so it may be helpful for learners to work in pairs. Each learner could set up a protected system and then create a test plan for that system. Learners should then test and review each other's protected system following the given test plan. This may help them to be more objective and critical of the degree to which the system is protected and the usability of the protected system. Learners could also use this experience to help them when considering how they could enhance their own protected systems.
- Learners should maintain a diary of the various practical activities that they complete in their lessons and the feedback they receive. They can then use this

information when they start work on their assignment and can no longer receive detailed guidance from you.

In contrast to *Unit 8: Business Applications of Social Media* where the skills, knowledge and behaviours should be discussed by the group from an external perspective (outside the organisation), in this unit they look inward and at the internal customers within the organisation. They need to know that in a computing/IT role they may well come into contact with most operational departments in an organisation and with most levels of staff from the newest junior to the Chief Executive. Learners should understand that large parts of computing are about process, documentation and professionalism. You should discuss what it means to be professional and why this is important in the industry.

- Ensure that learners understand how to fulfil the assessment criteria for the pass, merit and distinction grades.

Details of links to other BTEC units and qualifications, and to other relevant units/qualifications

Pearson BTEC Level 3 Nationals in Computing (NQF):

- *Unit 6: IT Systems Security*
- *Unit 9: The Impact of Computing*
- *Unit 19: Computer Networking*
- *Unit 20: Managing and Supporting Systems*
- *Unit 29: Network Operating Systems*
- *Unit 30: Communication Technologies*

Resources

In addition to the resources listed below, publishers are likely to produce Pearson-endorsed textbooks that support this unit of the BTEC Nationals in Computing. Check the Pearson website (http://qualifications.pearson.com/en/support/published-resources.html) for more information as titles achieve endorsement.

Websites

- www.bbc.co.uk/news/technology
  The BBC News Technology section has technology news, including cases of significant cyber-attacks.
- http://ico.org.uk/
  The Information Commissioner’s Office website gives case studies of actions taken under the Data Protection Act.
- http://home.mcafee.com/advicecenter/
  McAfee’s security advice centre has useful and up-to-date information on security, virus attacks and viruses, written in a reasonably accessible manner.
- www.microsoft.com/security/
  Microsoft's security advice centre features a regularly updated blog and FAQ on security issues.
- http://uk.norton.com/security-center/
  Norton’s security centre has articles on security, spam email, software piracy etc.
- http://www.bletchleypark.org.uk/
  Bletchley Park, the national Museum of Computing and wartime code-breaking centre.
- www.virtualbox.org
  VirtualBox® is a free open-source product that allows you to install a software-emulated virtual PC.

Videos

- www.youtube.com
  Search for video presentations on public key encryption: