Lesson plan

|  |
| --- |
| **Topic 6 Access control, backup and recovery** |
| Learning Objectives:   * Describe physical access control techniques for protecting data and systems * Describe processes and implications of techniques and procedures for protecting data and systems:   + File permissions   + Access levels * Backup and recovery procedures |
| Content |
| Starter  PowerPoint Guide:  Topic 6 Access control, backup and recovery  Ask the class what type of access controls they have on their smartphones. Can some students demonstrate different methods, for instance PIN lock, pattern lock, password lock, fingerprint sensing system?  You could show the following video: Seven essential steps to secure your device <https://www.youtube.com/watch?v=xWEFju0Sg1E> (2 minutes)  The Starter slide lists some of the suggestions given in the video.  Main  Physical access control  Elicit ideas from students on how the area around a building could be secured. Suggestions are given on the next slide.  Case study: Toll roads  Students should consider how toll roads now work as a physical access control. RFID payment cards are used, or automatic number plate recognition (ANPR). Once the payment is received or the number plate authenticated the barrier opens. Many toll roads have removed barriers and relied on online payment systems and ANPR. Examples are the Dartford Crossing bridge and tunnels (2014) and the Mersey Gateway Bridge (2017).  Authentication factors  Take students though these. Many students may have heard of the expression ‘two-factor authentication’. This doesn’t mean two passwords. It means two different factors/types of authentication have been used.  Case study: Payment cards  Discuss with students the different ways in which payment cards can be used. Some may not have seen swipe and signature used and need further explanation. Discuss also the advantages and disadvantages of each method. How could they be hacked? Some answers to the questions are given on the following slide.  Ask students to complete **Task 1** on **Worksheet 6**.  Topic 6 Worksheet 6  Topic 6 Worksheet 6 Answers  Fingerprint recognition and setting up biometrics  Discuss fingerprint recognition with the students. Students may be unaware that the full fingerprint is normally not stored but key parts of it known as ‘minutiae’. This is in an attempt to prevent the full fingerprint being stolen, however, in some cases the original fingerprints have been reconstructed. Take students through how biometrics are set up. You may like to have a student demonstrate how fingerprints are added to their device.  Advantages of biometrics and disadvantages of biometrics  Elicit advantages and disadvantages from students. Some answers are given on each subsequent slide.  Case study: Passport control  Have any of the students used a face scanner at an airport to open a barrier? It can be a slow process if the person in front is having difficulty using it. A useful website is  <https://biometrictoday.com/10-advantages-disadvantages-biometrics-technology/>  Automatic passport control systems use a chip on the passport (something you have) with facial recognition (something you are) which is two-factor authentication.  Ask students to do **Task 2** and **Task 3** on **Worksheet 6**.  Topic 6 Worksheet 6  Topic 6 Worksheet 6 Answers  File permissions and access rights  File permissions usually have three states (read / write / execute) with users to have a combination of rights to each file. Most schools will allow read/write access to user’s own area with read and/or write access to shared areas. Software programs will have execute rights. File permissions can be set up differently for each user and also groups of users. So, an individual student may have access to their files along with a technician and possibly teacher. A group of students may have read access to a shared area on the system.  File permissions in Word  Students may be familiar with the fact that Word documents may have permissions attached to them. These include making a file **read only** or the ability to **restrict editing**.  Access levels  Users using software may be given different levels of access. The example on the slide is of company financial software. Other software may contain different levels of access. For instance, a network administrator may be able to run any program on the system whilst a student will have limited programs they run. Access levels to the internet and websites can also be restricted.  The final topic in this lesson is **Backup and recovery** procedures. Ask students if they have ever lost an hour’s worth of work or more. How annoying is that? How about losing three months’ worth of project work?  For a company, losing days or weeks’ worth of data can be devastating. A watertight backup policy and a recovery procedure to go with it are essential. Statistics show that most companies who lose their data for 10 days or more go bankrupt within a year.  Backup  Every organisation needs to back up its data at least once a day. Some organisations backup continuously by writing simultaneously to two or more storage devices in different physical locations. A bank, for example, cannot afford to lose a single transaction. Booking systems for airlines, trains, theatres, etc. must back up data continuously.  The 3-2-1 rule  This rule (or more accurately, guideline) says that an organisation should always have three copies of its data, on two different types of storage with one copy offline.  Types of backup  Full backups and incremental backups are discussed. Most companies will use a combination of these with regular full backups perhaps once a week and incremental for each day of the week.  Restoring files from backup  The time and complexity of restoring files will depend on how much data has been lost, and over what time period. Sometimes a few days or even weeks can elapse before a data loss is detected. A full back up on a hard disk may be able to restore a file within seconds. An incremental backup on a tape drive may take a long time to obtain the tape and then find the location of the file on the tape.  Cloud storage and backups  Organisations and individuals who use Cloud storage for all their data can be confident that it is automatically backed up and retrievable in the event of a disaster. Do students use OneDrive, Dropbox or Google Drive? Where is the data accessible on their smartphones held? What happens if they lose their smartphones?  Many companies hold all their data files in the Cloud, where it can be accessed by employees or consultants working remotely.  Disaster recovery plan  A disaster such as a fire, flood theft or virus can cripple an organisation, so it is therefore essential that plans are in place to deal with such an event. Careful thought needs to be given to what could potentially be lost (hardware, software, data), who is going to be the person responsible for implementing the plan and what procedures they need to follow.  Benefits of a disaster recovery plan  Benefits of detailed advance planning are outlined. Hardware as well as software may be destroyed, premises made unusable. A useful reference is: <https://en.wikipedia.org/wiki/Disaster_recovery_plan>  Implications of data loss  If a disaster such as a fire or flood occurs, implications are far-reaching. Some of these are described on this slide.  Ask students to complete **Task 4** and **Task 5** on **Worksheet 6**.  Plenary  Ask students to come up with questions about the topics given to recap the lesson.  Hand out **Homework 6**.  Topic 6 Homework 6  Topic 6 Homework 6 Answers |