Lesson plan

|  |
| --- |
| **Topic 3 Methods of protecting data** |
| **Learning Objectives:**   * Describe the features, characteristics and implications of using antivirus software to protect data * Describe the process and implications of using passwords for protecting data and systems * Describe the features, characteristics and implications of using firewalls to protect data |
| Content |
| Starter  PowerPoint Guide: Topic 3 Methods of protecting data  Ask students to consider what types of malware antivirus software protects against and also to name companies that make antivirus software. The following slide shows answers.  Main  Protecting against viruses  Students may not realise how important it is to install the latest operating software updates when they are offered. New security weaknesses discovered by software companies such as Google and Microsoft are closed using “patches” which may be, but are not always, automatically installed. The user may be asked if they wish to install a new patch.  Case study: iOS 12  This case study shows some of the security updates made when upgrading to iOS 12. Failure to update the operating system leaves users open to these security risks.  A full list of the security flaws that the update fixes are given at:  <https://support.apple.com/en-gb/HT209106>  How does anti-virus software work?  A brief overview of how anti-virus software works is given here. Viruses are able to morph so that they are different sizes or may contain different code in an attempt to fool antivirus software. A heuristic analysis will look for features of the virus so that it can analyse further versions of it.  Detecting a virus  This slide shows how antivirus software works. First a copy of the virus is sent to the antivirus company. They will then analyse it to find parts which make it unique and can be added to their definition database. Once the definition database is updated on user computers they will be able to check files and see if it contains the virus definition. If so the virus has been found.  Real-time and full scans, quarantine and removal  Take students through these two slides which show the different types of scans which can be performed and how viruses are dealt with when they are discovered. Even though real-time scans of files may have been carried out, it is important that full scans are done often as they will have more up to date virus definitions to work from.  Impact of anti-virus software  The possible negative impacts are briefly described with further information here:  <http://www.itpro.co.uk/security/29665/does-antivirus-software-do-more-harm-than-good>  Ask students to complete **Task 1** and **Task 2** on **Worksheet 3**.  Topic 3 Worksheet 3  Topic 3 Worksheet 3 Answers  Protecting against hackers, validating and verification of a new password  The first and most basic protection is password protection using a strong password. Most websites now check that passwords are valid and meet a certain length and complexity. Users should be reminded that weak passwords can still be created. For example, if the password needs to be 8 or more characters and include a number “p455word” would still be insecure. The verification of passwords makes sure that users haven’t mistyped it when they first entered it.  Other verification methods  Email and online service providers may have verification methods to ensure that, if you are not using your normal computer, you are the genuine user.  Security question  The screen shows two methods of protection from hackers or spyware:   * Asking the user to enter only randomly selected characters from the password * Asking a security question and comparing the answer with the answer that the user gave on initial registration which is stored on the system   Foiling spyware  Another technique to prevent keystrokes being recorded by a hacker is to ask users to select letters and numbers rather than typing them in when entering a password or “memorable information”, an extra login step designed to strengthen security. This would foil a keylogger, but spyware could still take screenshots to establish which letter was pressed.  CAPTCHA  **“CAPCHA”** is a common technique which students will probably be familiar with. One problem with this is that sometimes humans can’t read the relevant letters. Alternatives need to be provided for those who use text to speech software. Often users are now asked to select different images – such as those that contain a car.  Most common passwords  Common passwords used will be added to password dictionaries. These passwords are particularly vulnerable and will be tried quickly in a dictionary attack.  Using a password manager  This is a useful piece of software for managing passwords. The advantage of using such a system is that all the passwords stored inside can be incredibly complicated and different from one another. This increases security when used on individual websites. However, the vulnerability of such a system is that if the main password is compromised then hackers have access to all passwords. Generally, it is advised that people make use of password managers for most passwords, however, those such as banking passwords should not be stored in them.  Threats from digital devices  Mobile phones and other portable devices are vulnerable to threats, especially if lost or stolen. Do all students have a lock on their phone? Have they changed the default PIN? The question asks about passwords that people often fail to change. A Wi-Fi router may be one example. These often have preinstalled passwords that are not changed. Whilst it is convenient for the password to be written on a home router, it is not very secure. In some cases, it may be possible to read through a window.  Always change the default  If a hacker can guess the PIN, they may be able to access voicemail remotely. And, of course, if the phone is lost or stolen, the data held on it is vulnerable. The phone hacking scandal was often as trivial as accessing a voicemail secured behind a PIN of 0000.  Ask students to complete **Task 3** and **Task 4** on **Worksheet 3**.  Keeping systems and data secure  Most computers are connected to the Internet, which leaves them vulnerable to attack. There are many solutions to these vulnerabilities. Some include training staff, using anti-virus software and updating computers. The remaining slides consider firewalls.  Firewall  Explain the function of firewalls as a device to prevent unauthorised access. They can be implemented in hardware (to protect a network) or software (to protect a single computer). The diagram shows a firewall implemented in hardware.  Ports  Any data going into or out of a computer or network will be directed to a specific port depending on the type of service it is for. Ports can be blocked to prevent them being attacked. The ports shown are used for the following: port 21 – FTP (file transfer), port 23 telnet (remote terminal), port 25 – SMTP (email sending), port 80 – HTTP (web pages), port 110 – POP3 (an older email standard).  A two-way firewall  This will also monitor outgoing communications and will block, for example, malware introduced on a memory stick, from getting on to the Internet.  Some organisations use firewalls to prevent employees sending certain types of emails or transmitting sensitive data outside of the network  Firewall in a home router  Usually a home router contains a built-in two-way hardware firewall.  Limitations of a firewall  Limitations are discussed on this slide.  Ask students to do **Task 5** on the **Worksheet 3**.  Plenary  This lesson has considered three areas. Students are likely to be able to make significant improvements to the security of their devices and home networks. Ask them to consider these in a discussion and then make the necessary improvements when they go home.  Hand out **Homework 3**.  Topic 3 Homework 3  Topic 3 Homework 3 Answers |