

**SAMPLE ASSESSMENT MATERIAL**

**Level 3 Cambridge Technical in IT**

**05839/05840/05841/05842/05877**

**Unit 3 Cyber Security**

**Date – Monday 21 May 2018 – Morning**

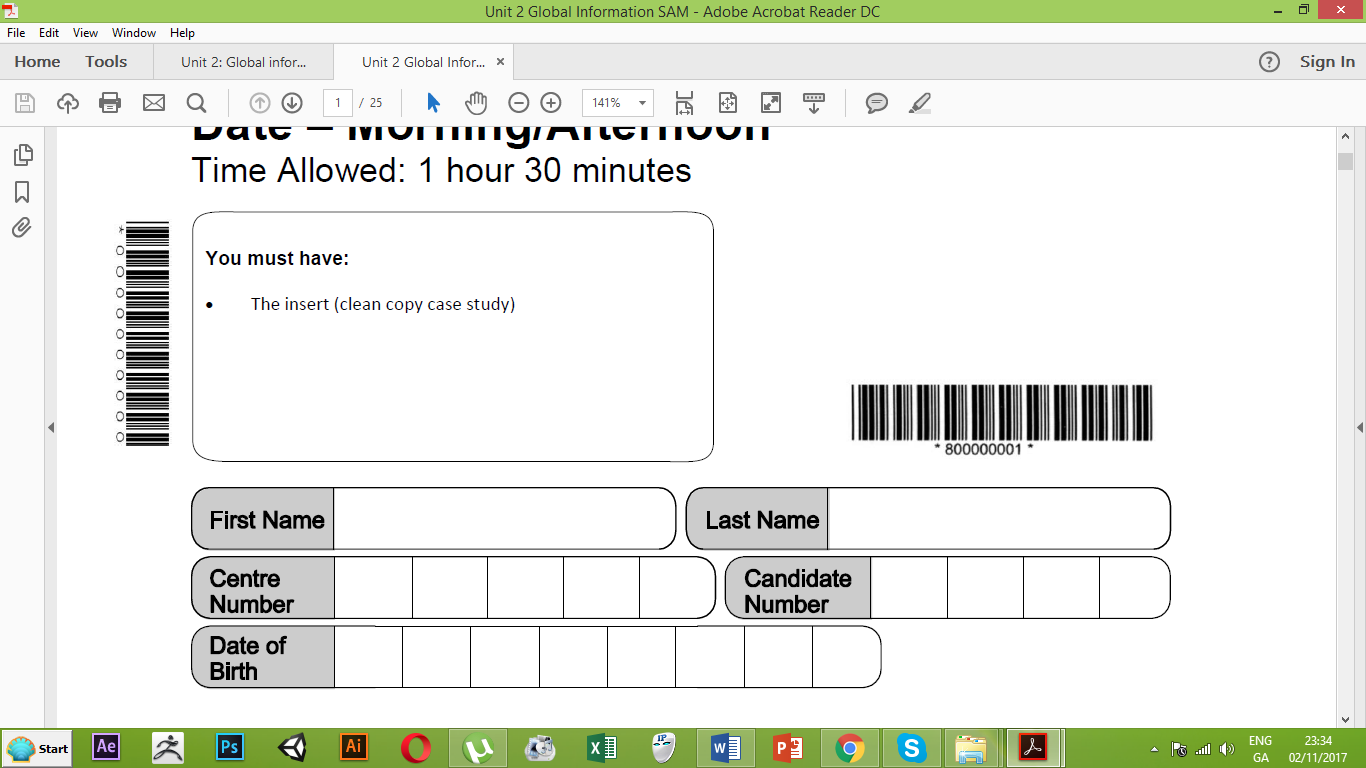
Time Allowed: 1 hour 30 minutes

****

You must have:

The insert (clean copy case study)

****



**INSTRUCTIONS**

* Use black ink.
* Complete the boxes above with your name, centre number and candidate number.
* Answer **all** the questions.
* Write your answer to each question in the space provided.
* Do **not** write in the bar codes.

**INFORMATION**

* You should make yourself familiar with the pre-release material before you take the examination.
* You must not take notes into the examination.
* A clean copy of this pre-release material will be given to you with the question paper.
* You must not take this copy of the pre-release material into the examination.
* This document consists of 4 pages. Any blank pages are indicated.

**Digital Personal Assistant**

**Background**

A digital personal assistant is a device that responds to vocal commands. It is activated by a keyword and will then run a command based on the vocal input from the user. Commands can include, amongst other things:

* web searches;
* playing music;
* creating/amending shopping lists;
* creating/amending to do lists;
* purchasing items from the web.

**Mr. Daka**

Mr. Daka lives at home with his wife and two teenage children. He is interested in new technologies and their ability to automate everyday tasks.

Mr. Daka has purchased a digital personal assistant for his home. He has integrated the device into his home automation system. This has included:

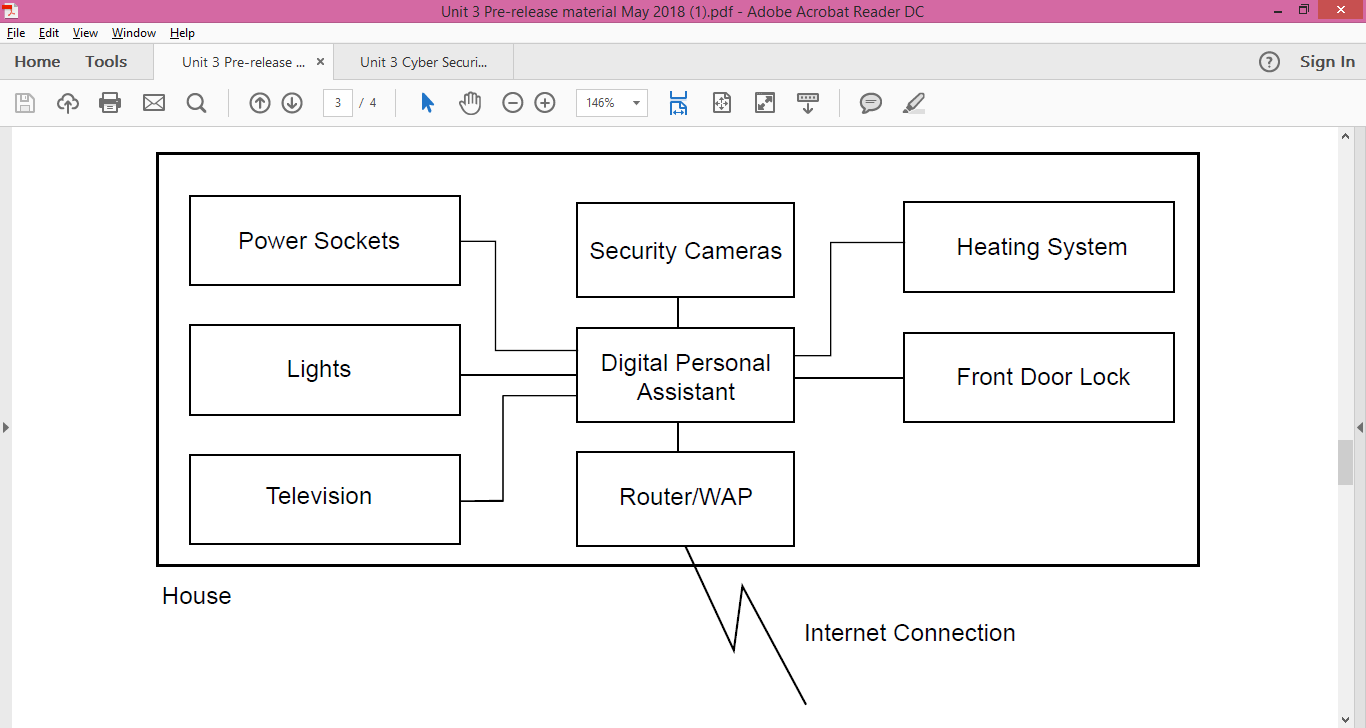
* security cameras;
* heating system;
* home entertainment systems;
* lights and power sockets;
* home locking mechanisms.

**Set Up**

Mr. Daka has a single internet connection into the house which plugs into a hybrid router, combining routing, switching and a wireless access point (WAP) into a single device, given to him by his internet service provider.

Mr. Daka has set the system up so that he can control his devices and change settings through a variety of apps on his smartphone. This allows him to perform tasks such as turning lights on and off, adjusting heating, opening the front door and viewing security cameras when he is away from his home.

**Diagram of Digital Personal Assistant and Home Automation Integration**



To prepare for the examination, you should research the following themes:

* information needed by an attacker to gain access to the digital personal assistant and connected devices;
* different devices that can be connected in a home automation system and the implications for each type of device of being attacked;
* methods that could be used to exploit and mitigate against vulnerabilities in the different connected devices;
* different types of attackers who might want to access the digital personal assistant and their motivations.

**Section A**

**This section relates to the case study.**

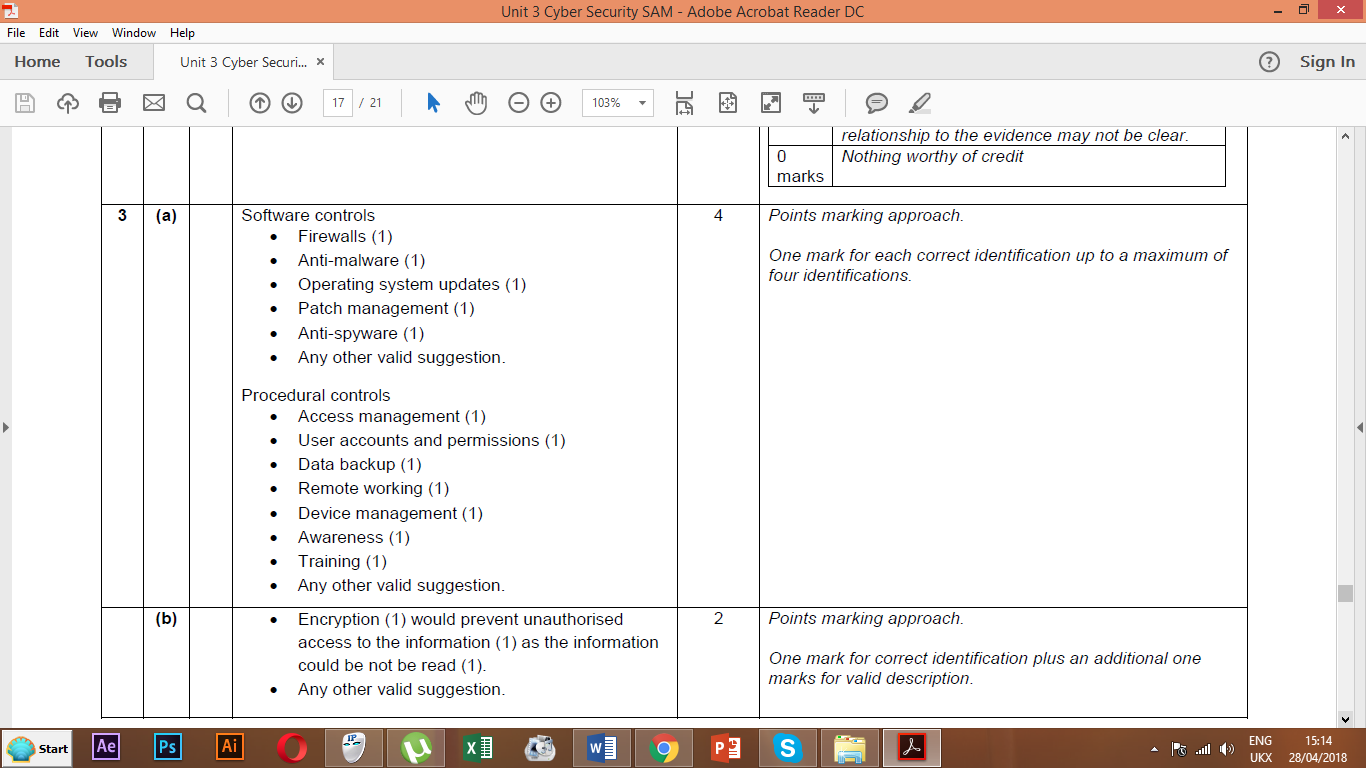
1. **(a)** Mr. Daka uses a keyword to initiate the Personal Digital Assistant. Describe two ways in which this keyword can be secured.  
   Method 1: making the keyword personal to him and not something easy to guess, using alpha numeric characters if it is typed or multiple words if it is spoken.  
   Method 2: Changing the keyword every short period of time in order to reduce down continuous guessing, alternate characters or making it multiple upper, lower, numeric and character based. **[4]**
2. Identify two types of attacker, working alone, who would be interested in compromising the control system of the Personal Assistant.  
   1: Hacker  
   2: Burglar (also malware agent, thief, rival company, scammer etc. Anyone will do as long as it can be justified in the follow up question. [2]
3. For one of the attackers, identified in part (c)(i), identify two of their characteristics.  
   Name of attacker: Hacker

1. uses remote access, hacking tools or brute force program to infiltrate network.

2. Likely to give up if the protection is too complex, will try to guess or use other methods to gain a fraction of the password to improve success rate. [2]

1. The risk to the integrity of the security cameras will be a priority in this set-up, but what are the risks to Mr. Daka concerning web search history.  
   Use web search history it may be possible for a hacker or scammer to access login names and passwords to access the computer, email login to help reset the password, confidential information used on sites to blackmail or use against Mr. Daka. Can also be used to add software, redirects of control browsing. [3]
2. Integrating the heating system involves linking sensors, ADC/DAC converters and the control device. In terms of the heating system, describe the function of each of these.  
   Sensors: These include heat sensors that determine the room temperature against the user pre-set value, if the temperature is above or below the required level, the system will act.  
   ADC/DAC: This takes the signal from Analog (the temperature thermometer) converts it to digital and communicated this to the control device. The returned signal reverses the digital to analog instruction forcing something physical to occur such as the heater starting or stopping.  
   Control Device: this is the physical device that is instructed to act on digital or analog controls such as the heater or air-con. The control device matches the value set against it and is moderated by the sensor. **[6]**
3. Discuss possible impacts on the home locking system being breached.  
   Either the family will be locked out of the house and the system will need to be reset, or the system will be compromised leaving the house open for burgling. This can lead to an expense in resetting the device, newer security measures placed to reduce the threat from re-occurring. **[3]**
4. Recommend two software controls and two procedural controls that Mr. Daka should use.  
   Write your answers in the box below:

|  |  |
| --- | --- |
| Software Controls | Procedural Controls |
| 1: Updating the software system to reduce known security flaws | 1: Testing the system on a regular basis to make sure the physical controls are still functioning. |
| 2: Resetting passwords over a period of time to reduce the threat of the security being guessed. | 2: Having the system checked or serviced on a regular basis to maintain optimum efficiency. |

**[4]**

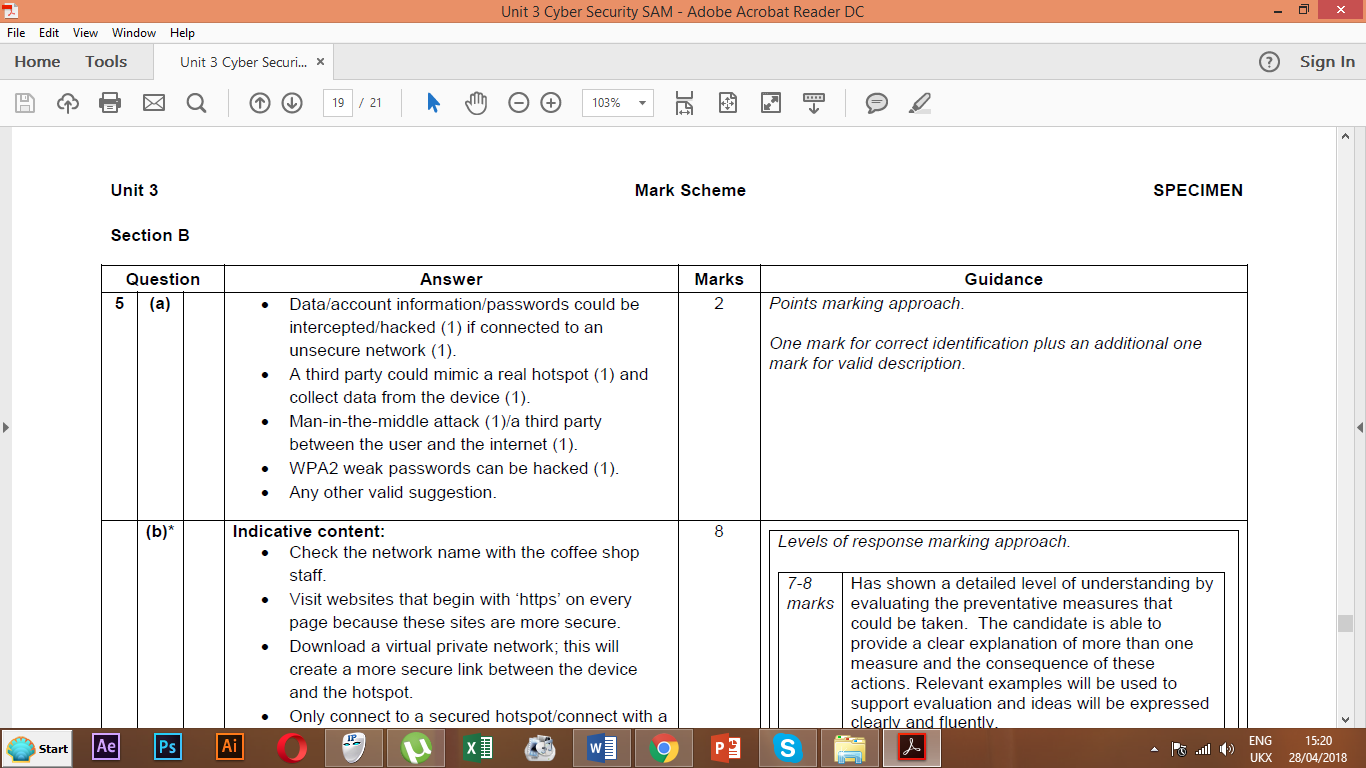
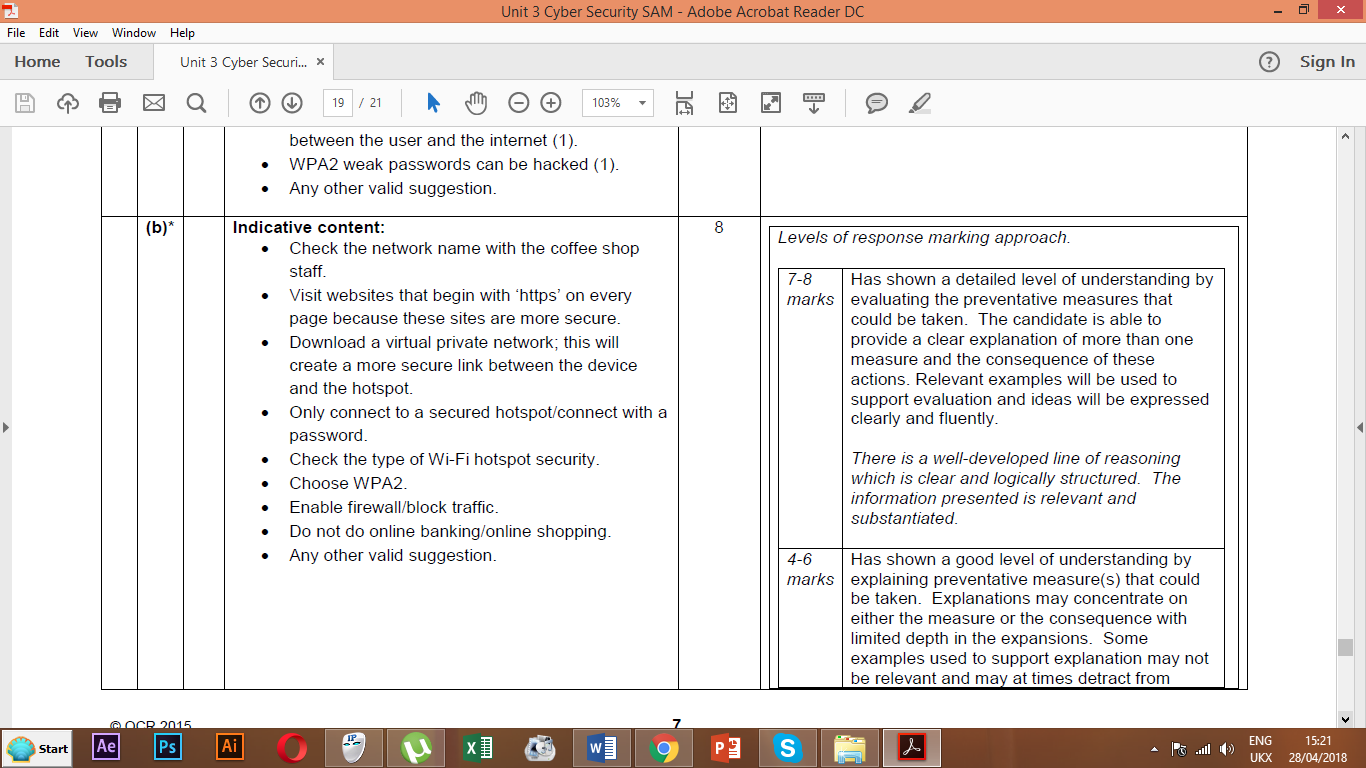
1. (a) Choose one category from the list below that describes the incident of the stolen external drive described in the case study.  
   Enter a tick in the box next to your choice.

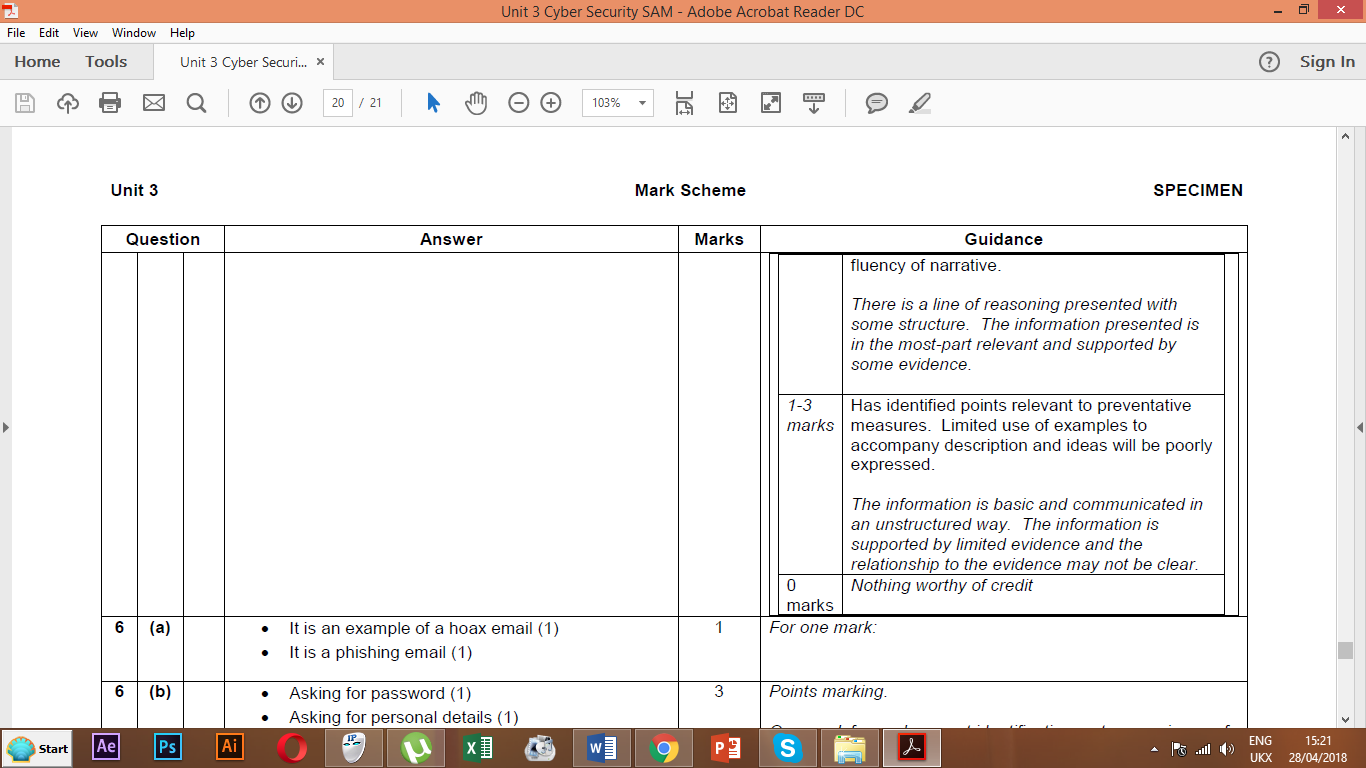
|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Security Cameras | Heating Systems | Home Entertainment Systems | Lights and Power Sockets | Home Locking Mechanisms |
| Critical | X |  |  |  | X |
| Significant |  | X |  | X |  |
| Minor |  |  |  |  |  |
| Negligable |  |  | X |  |  |

**[3]**

1. (b) Justify your choice of category Lights and Power Sockets.  
   The worst that can happen if the lights are compromised is that they may not work during a time when needed, such as a fire or burglary but they are not essential at all times of the day and not necessary to take down the whole system to have them changed or repaired/ Similarly electric sockets might be overused through compromise but this will cause a circuit breaker or power cut which is significant for the integrity of the whole system but not critical. **[2]**

**Section B**

1. Describe one potential cyber security issue associated with Mr. Daka connecting his tablet or laptop to the hybrid router if it had an unsecured WAP hotspot.  
   The tablet may contain confidential information, on an unsecured router the tablet could be accessed through the wi-fi and searched for passwords of confidential information, spyware, malware or a key logger could be placed on the device which could lead to more serious risks to the system integrity. **[2]**
2. Evaluate the preventative measures you could take when connecting your tablet or laptop to an unsecured Wi-Fi hotspot.  
   Software updates including virus definition files, encryption placed on confidential documents, firewall installed on the laptop, secure login name and password on the device and on sites visited, added biometric security on the laptop such as finger print or facial recognition. VPN or proxy could also be mentioned. **[4]**  
   



1. If Mr. Daka lost his Smartphone, what protocols could he have put in place on his Smartphone in order to protect his home Digital Personal System?  
   Protocol 1: keypad lock  
   Protocol 2: Email and personal pages might not have the auto connect feature turned on so they will require logging in each time.  
   Protocol 3: Biometric security could be set up, or the phone may need to login in to the home system through a secure password option with a three guess lockout that would allow Mr. Daka to change the home system password in time. **[3]**
2. Describe two additional devices that could be added to the home automation system, and describe the security risk they would need to be protected from.  
   System 1: Bluetooth devices such as cookers and fridges – security risks could include powering off or on and losing food.  
   System 2: Car, garage doors, greenhouse controls, ventilation, anything that could contain a sensor can be controlled and the security risk will be similar, turning on or off, using power, overloading the plugs etc. **[4]**
3. Digital Personal Assistants have vulnerabilities from cloning devices, hacking tools and WAP password sniffers. Describe each of these methods that could be used to exploit the system and for each describe a method to mitigate against vulnerabilities in the different connected devices;  
   Hacking Tools: Hacking tools could be used to brute force guess a password in order for the hacker to gain access to the system. Preventative measures include difficult passwords, alpha numeric and biometric systems.  
   Cloning tools: A device used to copy the ability of a similar device in order to control the same functions such as a car cloner to copy a card that could be used to access the door, or a fob cloner to allow a thief access through security measures. Preventative measure include being physically careful, using biometric fobs or adding in additional security to cloned devices such as a numeric password.   
   WIFI Sniffers: A software or hardware tool used to run through a series of password guesses to get onto a wi-fi network. Once there, it can be used to hotspot or to network access another device with the purpose of infiltrating, stealing or key stroking a system. Can also steal broadband width. Preventative measures include strong passwords, firewalls and regularly changing passwords. **[6]**
4. Describe the damage the following forms of attack could do to the operational function of the Router/WAP.

DDOS: Denial of service attack will cause a network or system to spend a lot of time dealing with the problem in order to stop dealing with other things, causing network outage or slowdown.   
Malware: Software installed onto a machine in order to allow other software access to steal passwords, or track users, can be nuisance or malicious, can cause a machine to slow down or crash altogether with the intention of hurting a business function.

Script Kiddie: this is when a person who uses existing computer scripts or codes to hack into computers, lacking the expertise to write their own, using known system vulnerabilities to gain access to a system. It will possibly allow a hacker to access the network or control system in order to compromise its functions.  
Piggybacking: Allows a remote user access to the broadband or traffic to free ride or steal broadband width. Will slow a network down and can be used to perform illegal activities without being blamed. **[8]**

**All answers must be phrased in context to this system.**

1. The following forms of prevention have been included in the software of the Digital personal Assistant, Describe their function.  
   Anomaly Based Recognition: This is a routine that is set to check on the system integrity by checking each performed routine, its regularity and purpose to verify if the instructions were valid or part of a hacking routine. If the routine was not valid, it will be added to a block list to stop it from performing again.  
   Account Lockout: Designed to allow the system to hold off on logging in if a series of failed attempts have been made, can be set up to inform the owner of the failed attempts with an intention of getting them back on through email or phone verification.  
   Patch Management: A program that regularly checks against the company server if any software patches have been created to reduce down vulnerabilities, if there has, the software will then download and apply the patch at a given time when the system is not being used in order to reduce threats.  
   Host Firewall: This is the firewall of the company, not Mr. Daka and will be the first line of defence by the company for its own information, checking login attempts and control device access for legitimacy before allowing the legitimate user access to downloads and patches of for user support. **[8]**

**Marks out of 60: \_\_\_\_\_\_\_\_\_**

**Grade: \_\_\_\_\_\_\_\_\_**

**Grade Boundaries based on June 2017:   
Pass - >22 Merit - >33 Distinction – >45**