# Answers

Task 1

1. Hotels often store personal data about their guests.

(a) Give **five** items of personal data that are likely to be stored about guests on a hotel’s computer systems.

Name, surname, passport number, passport photo page details, date of birth, address, room number, email address, contact number, payment card details

(b) Describe how a phishing attack may be able to get personal details about a hotel’s guests.

* A phishing email is sent which encourages a hotel employee to visit a website and enter their password to a system.
* The site looks like a real site the user would use, but is in fact owned by the hacker.
* The site remembers the login details/password of the user.
* The hacker can now use these details to log in to a system owned by the hotel.
* Having gained access to the hotel system they will be able to find guests personal data.

There is an alternative strategy of phoning an employee and asking them for their details. For example, a hacker could pretend to be from an IT support company and request the user’s username and password to solve an issue they are having with the account. The could then use these details to log in to the system.

(c) The data about guests could lead to identity fraud. Give **three** ways in which a fraud may occur.

* Buy products using bank cards
* Open a bank account in the guest’s name
* Obtain an overdraft
* Take out a credit card
* Take out a mobile phone contract / a contract for a service

(d) What are three impacts to the business and individual of this fraud occurring?

Impacts on individuals:

* The customer may have debts which they can’t pay or aren’t aware of.
* If these debts aren’t paid, their credit rating could be damaged.
* Even if they do pay the debts, their credit rating may be damaged by having so many cards/loans/credit checks.
* The customer may have to spend a large amount of time proving the debts aren’t theirs
* They may suffer from stress/anxiety as a result.
* If problems aren’t resolved before applying for a mortgage/remortgage/rental property, the customer may find it hard to stay in the house/rent a new house.

Impacts on the business:

* Loss of reputation
* Pay compensation
* Pay for better training for staff
* Pay to fix any holes in security of their systems
* Pay fines to the ICO (Information Commissioner’s Office)
* Reduced bookings due to loss of reputation which could lead to the business needing to close

Task 2

Look up the following website, or search for ***Facebook phishing scams***:

<https://www.hoax-slayer.net/4-scams-that-all-facebook-users-should-know-about/>

Describe some of the possible consequences to you and your Facebook friends of falling for such a scam.

You may reveal your email account password, your credit card details, and a lot of other personal information. The criminals can then use your credit card to make fraudulent purchases, or even steal your identity.

The criminals will have the email addresses of all your friends and they will receive the same scamming email, this time even more convincing as they will know the name of the person they are scamming.

Task 3

1. Research and write notes on the impact that threats to data, information and systems can have on

(a) **Individuals**

See, for example:

<https://www.forbes.com/sites/quora/2018/01/30/how-cyberattacks-will-affect-the-average-person-in-2018/#5ef196655efa>

**Impact on the individual:**

Identity theft, financial losses, reputational damage.

Email accounts, social media sites and other personal information may be compromised.

Attackers are honing their skills to create cyber-attacks containing a mixture of real and false information, tailored to individuals and sent out via emails and social media. Global crises, social unrest, and boycotts occurred in 2017 as a result of cyberattack combined with disinformation.

(b) **Organisations**

See, for example:

<https://www.nibusinessinfo.co.uk/content/impact-cyber-attack-your-business>

**Impact on businesses:** Financial costs, reputational damage, legal consequences, bankruptcy

(c) Now make a presentation on what you have found out.

Task 4

Carry out some research on the Internet to find out about the economic impact on companies of employees losing their laptops. How can the impact be reduced?

There are lots of websites… get the students to look up “impact of losing laptop” in a search engine.

Laptops often contain corporate information, customer data and intellectual property, which, if unprotected, could undermine competitive advantage or force the organization to publicly acknowledge the possibility of a data breach.

Such incidents may result in huge costs in notifying customers, fines for noncompliance of the Data Protection Act, possible class action lawsuits and brand damage.

<http://www.cio.com/article/2443546/it-strategy/how-to-minimize-the-impact-of-laptop-theft.html>

Task 5

Answer the following questions about a Denial of Service attack.

(a) What is a DoS attack?

A DoS attack is an attempt to make a machine or network unavailable to its intended users. Attackers will flood the connection to the server with unnecessary requests.

(b) Who is typically targeted?

Typically, large organisations are attacked, but all users of the site are affected as the site slows down or becomes unavailable

(c) What are the consequences to an organisation of a DoS attack?

The impact could range from a minor annoyance from disrupted services to experiencing entire websites, applications, or even an entire business being taken offline.

With more and more businesses running software in the cloud, a loss of productivity could be huge with users of services that are under attack.

Websites with useful further information:

https://www.csoonline.com/article/3020292/cyber-attacks-espionage/ddos-attack-on-bbc-may-have-been-biggest-in-history.html

<https://www.csoonline.com/article/3222095/network-security/ddos-explained-how-denial-of-service-attacks-are-evolving.html>

**Task 6**

An Austrian hotel suffered four ransomware attacks between 2016 and January 2017.

Read the following BBC news report about the attack: <https://www.bbc.co.uk/news/business-42352326> and answer the following questions based on it.

(a) How was the ransomware attack initiated?

A bill was received suggesting it was from Telekom Austria. By clicking a link in the bill, the ransomware will have been downloaded and executed on the computer.

(b) What did the ransomware attack hold ransom?

Files on the computer were encrypted and door keys became unusable

(c) How much ransom needed to be paid?

Two bitcoins – at the time about £1,406/€1,600

(d) What actions have been taken to reduce the risks of this happening again?

Firewalls and new antivirus software have been installed

Staff have been trained to recognise phishing emails

Electronic keys have been replaced with metal keys

(e) The BBC article reports that the “hotel’s electronic door locks… were hacked for ransom” The headline also states “Locked out”.

 Read the article at: <https://www.wired.co.uk/article/austria-hotel-ransomware-true-doors-lock-hackers>

 What is a more accurate description of what happened with respect to rooms?

The room locks were not themselves compromised by the ransomware attack

Guests were able to use the locks as normal with RFID key cards. They could enter and exit room doors

The ransomware encrypted the computer systems of the hotel so that new key cards couldn’t be programmed. This meant that any customers arriving after the ransomware attack, or any customer who lost their key, could not be given a key to their room