1598230452

Unit 8 - Ecommerce

Task 2 Consumer Guide

Part 1

* Data Protection Act 1998

This act provides rules and regulations as to how personal data should be handled. Also, people have the right to know what kind of data is being held about them. Personal data can be kept both digitally and as a paper based record. This act in the UK is regulated by the information commissioner whom can be contacted by anyone who has a problem regarding their personal data.

Firstly, for anyone to be able to process personal data they must register with the DPA registrar and strictly follow eight principles. These principles ensure that data is:

* Data must be kept fairly and legally
* Data must be obtained for a clear and limited purposes
* Data must be adequate, relevant & not excessive
* Data must be accurate and kept up to date
* Data must not be kept for longer than necessary
* Data must be processed in line with human rights
* Data must be kept secure
* Data must not be transferred to other countries without protection
* Computer Misuse Act 1990

This act compromises of three main offences:

* The unauthorised access to any computer program. One way this can be done is through hacking or simply using a computer that has been kept logged on. A second way is altering a program or data as well as altering data held on paper.
* The unauthorised access with intent to commit a serious crime. This means obtaining unauthorised information with the idea to sell the data on for example. Access can be gained through introducing a Trojan to the system or creating a backdoor to it.
* The unauthorised modification of computer contents. Such content can include the operation of a computer, a program or the reliability of data. Furthermore, this will also include the prevention of access to a program or data. This is most commonly done through viruses as well destroying and modifying a user’s files.

Breaking the computer misuse act can actually result in anywhere from a penalty to a prison sentence.

* Consumer Credit Act 1974

This act protects customers who use a credit card or a loan to pay for goods and services of up to £25,000. The act protects customers by stating that if the payment cannot be paid then the business will still receive the money and then send out the goods or service to the customer.

Furthermore, the act also states that if the customer changes their mind about the purchase of a product then there is a 14 day period in which the customer can ask for a refund.

* Freedom of Information Act 2000

This act is associated with the right for people to have access to official information published by public authorities hence the name freedom of information. Official information is often found in places such as the police, NHS & schools. The information must be processed and given to said person within 20 days or else it is seen as breaching the act. There are some cases in which companies can refuse to provide the information given it is not related to the act. For example, the NHS could not provide someone within patient data because it is personal data which must be protected under the data protection act.

These public authorities are often wary to share this information as it can be used as a weapon to attack the authority.

* Copyright, Designs & Patents Act 1988

This act protects creator’s original work as well as giving them the right to seek action against any damages sustained. In terms of e-commerce, one way in which this act will protect the website is against images on the website. For example, a supermarkets e-commerce website may contain images of the groceries they sell and if these are found elsewhere then the supermarket can seek action against those responsible for plagiarising the images. Also, this act can protect original work of up to a whole website. This works by looking at the html code of the website for any similarities in the code.

The act states that original work can be obtained from the creator but permission must be asked as well as explicitly quoting the source of the work.

Part 2

1. Changing customer perspective

One of the biggest issues which affect footfall of e-commerce websites is the fact that customers have a sceptical view of online shopping. This is because articles are published in the news warning people about credit card details being stolen, undelivered products and identity theft.

One way in which an e-commerce entity can change the perspective of customers is to promise good value of products and services. This means offering lower prices than at the high street stores and also products which are not available at the store.

A second way in which entities can change customer perspective is to make sure the website is very secure. Using a variety of methods such as anti-virus software, encryption and authentication will manage to keep any threats at bay. It is vital that entities make the website as secure as possible because there will be a large amount of personal data on the systems and if this got out it would lose customer trust and be seen as breaking the data protection act.

1. Impact on society as a whole

One impact on society that e-commerce has is the goods & services are available worldwide. This means that if a company only had stores in one country then customers would not need to fly overseas to get the products. Also these countries that otherwise wouldn’t be able to get the products would not need to battle the changes in time zones because the website is accessible 24/7.

Another impact on society which e-commerce has is the ability to ‘shop around’. There are price comparison websites which help society find the best deals on the web. Also, due to pure e-commerce businesses such as Amazon not needing to spend costs maintaining stores it means that they can sell products for cheaper and therefore customers also get the benefit of cheaper products.

1. Social impact due to speed of change

Despite the blow up of the internet and technology over the past 20 years there are still some people who have no or outdated technology meaning that these people cannot use e-commerce sites as an alternative. Additionally, this means that it is likely that traditional stores will still be running in years to come to accommodate for these small amount of people.

One reason why some people do not have access to these e-commerce sites is due to their income. If a family has a low income then they may find it hard to be able to afford a computer and have an internet connection installed by an ISP. This creates a social divide as e-commerce can be seen as a ‘luxury item’ and only available to middle class and above.

1. Bricks & clicks (integrating high street and online presence)

A brick and click organisation can be defined as an organisation which both has a presence online as well as having physical stores. Examples of these organisations include TESCO and HMV.

As mentioned having both a website and a store allows the whole of society to be able to purchase products from the organisation. Again, people who live overseas can purchase the products and those who don’t have internet can go to the stores.

One disadvantage of having a brick and click organisation is that it means the organisation will find it hard to cut the prices online. This is because they need money to be able to maintain the stores (rent, electricity & maintenance). Pure online businesses such as Amazon do not need to worry about this and can therefore change the prices with ease. This means that potential customers will be more likely to go to Amazon because one of the main factors that they look for when buying products is the price of them. In turn, brick and click organisations lose out on potential sales which is the main fundamental for a business to stay afloat.

Part 3

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Security Issue | Effect of security threat | Prevention method used | Prevention methods effect on performance | Law violated if threat is successful |
| Hacker | A hacker is someone who can get into a computer system despite having unauthorised access with the intent of causing damage to the system. The hacker may choose to manipulate data, slow down the system or crash the system. | One way in which we can stop this from happening is by putting a firewall in place. The firewall will block, monitor and restrict traffic to specific ports meaning that anyone who is unfamiliar, likely the hacker, can be blocked out using certain settings.  Another prevention method for a hacker would be to implement levels of access. This would mean that certain documents and files can be set to read only. Read only means that you cannot edit the file unless you have the authentication needed to edit it. This would mean that the hacker would need to spend more time getting into the file which in turn may deter them off gaining access to that certain file. However, this can slow down the computer system because it needs to constantly monitor and store what files can be accessed by what accounts.  A third prevention method to stop hackers gaining access to a computer system is by using SSL, also known as encryption. Encryption can be defined as changing the format of data and then using a key to help decode it. Without this key it will become very hard to decode which is good because the hacker will not have access to this key. However this can slow down a website because the data needs to be decrypted first before it can display the webpage. | The firewall can slow down your computer system because it is constantly monitoring if a packet or device is allowed to connect when it has sent a request to connect. | Firstly, the hacker will be breaking the computer misuse act because they have gained access to the system without authorisation.  Also, the hacker could be breaking the data protection act if they choose to view or manipulate personal data of staff members or customers. |
| Denial of service | A denial of service attack can be explained by someone overloading a network by flooding it with requests which will cause it to crash or significantly slow down due to the amount of traffic hitting the network. People do this because of numerous reasons such as: to send a threat, expression of criticism or even just for fun. | One way in which an attack could be prevented is through a firewall. The main role of a firewall is to prevent unauthorized users from accessing a private network, such as the person planning the attack. The firewall will look at each individual packet and accept or reject based on user-defined rules. | However, as expected this is likely to slow down a download or request because the firewall will be checking so many packets before it can be received to perform the action. | A denial of service attack is seen as breaking the computer misuse act because the person has gained access to the system with the intent to bring the website down. |
| Viruses | A virus is a program or a piece of code which will cause harm to a computer if executed. Viruses find their way into computers by disguising the program or code as a game or image. Common effects that the virus can perform include corrupting data, removing data and crashing the system. | The most frequently used method of preventing viruses is anti-virus software. Antivirus software works by scanning the machines drives to see if any programs or code match any known software. Then the software will remove the program or code if requested by the user. | One effect on performance that antivirus software has is that it slows down the computer. Antivirus software is constantly updated as new viruses are created each day and therefore the software needs to know about the virus. In turn this builds up memory and therefore taking up hard drive space. | The use of viruses is firstly breaking the computer misuse act because unauthorised modification of computer material happens. Also the implementer of the virus may choose to view and modify personal data. This will be breaking the data protection act as one of the principles is to keep data secure. |
| Identity theft | Identity theft involves a thief who has stolen personal details of a person and will use these details for financial services such as applying for credit cards. The effect of identity theft is that when the money spent is being chased up the addresses of the victim will be used even though they are not in the wrong. | People should regularly check the payment transactions from their bank to check they aren’t any anomalies.  Also people should change their passwords and PINs quite often because the thief will not know the password. | The problem with using passwords is that they can be forgotten easily and therefore access to the system cannot be granted. Also, if the password is written down then it can be misplaced and fall into someone else’s hand. | The thief will be breaking the data protection act because they have gained access to personal data and therefore it is not used for the correct purpose. |

Part 4

PayPal is one of the most commonly used payment methods. PayPal allows user to load a set amount of money into an account to be able to purchase items from the internet. PayPal make their money by charging a small fee on each purchase. One pro of PayPal is that it is a very reputable payment method. This means that they have the trust of people in terms of being able to handle their information and therefore generate more people. One disadvantage of PayPal is that money can be ‘frozen’ in the middle of a transaction if they feel like someone is abusing the system. This means that the receiver of the money cannot gain access to it even though it should be theirs. This gets more and more of a problem when the amount of money frozen increases.

Net Banking is a platform which is used by customers which use internet banking which has preloaded customer information. One advantage of Net Banking is that they ensure that personal information will not be given to websites which seem untrustworthy. One disadvantage of Net Banking is the amount of information held on the system can be a large amount and if the system was to get hacked into then it could be catastrophic.

Electronic cheques actually allow users to pay with a cheque at a till and keep it because the transaction is done online. Electronic cheques are only usually supported with larger businesses that customers have an account with the company. One advantage of this method is the speed in which the transaction can be done. Paper-based cheques could take up to 28 days to clear whereas an electronic cheque could only take an hour or two. However, this can be a disadvantage to the person who is giving the money as they have no time to be able come up with the money as there is no float time.

NoChex is a relatively unknown payment method available to the world, NoChex is a small private company based in the UK which only employs 24 people. Usually, only small businesses use this payment method as this is their target audience. Advantages of NoChex include the speed of transaction, security and the ease of use. One disadvantage of NoChex is again the ability for NoChex to be able to freeze accounts and transactions which in turn has led to bad reviews. These bad reviews put off potential users and therefore it becomes an underused method.

A final payment method is Google Wallet. This method is very similar to PayPal in the way that it can be loaded with money and be used to make payments. A unique feature of Google Wallet which attracts customers is the fact that they offer an e-mail service in which money can be attached to an email which gives the system a personal touch. One advantage of Google Wallet is that no intruders have found their way in to the system to date which in turn means the customers trust and will continue to use the system. Another big advantage of Google Wallet is that it is a free payment method which gives it an edge over its close competitor, PayPal. However, very few websites allow users to make a payment through Google Wallet because PayPal is more commonly used and well known and seen as though they are similar PayPal is used.

In conclusion, the most suitable payment method from the ones listed above is PayPal in my opinion. As mentioned PayPal is the most common method and therefore it is highly likely that people have a PayPal account and other such businesses will have it for business transactions. All though a fee needs to be paid each time a payment is made it is only a small figure and all other methods but Google Wallet also charge a fee. In terms of the future it means that the businesses does not need to switch payment methods as this could cause problems with payments or payments not being able to be made during the switch period. Also if the business was to expand abroad then international payments could be made as PayPal is a worldwide service.