**P3 – Explain the security risks and protection mechanisms involved in website performance**

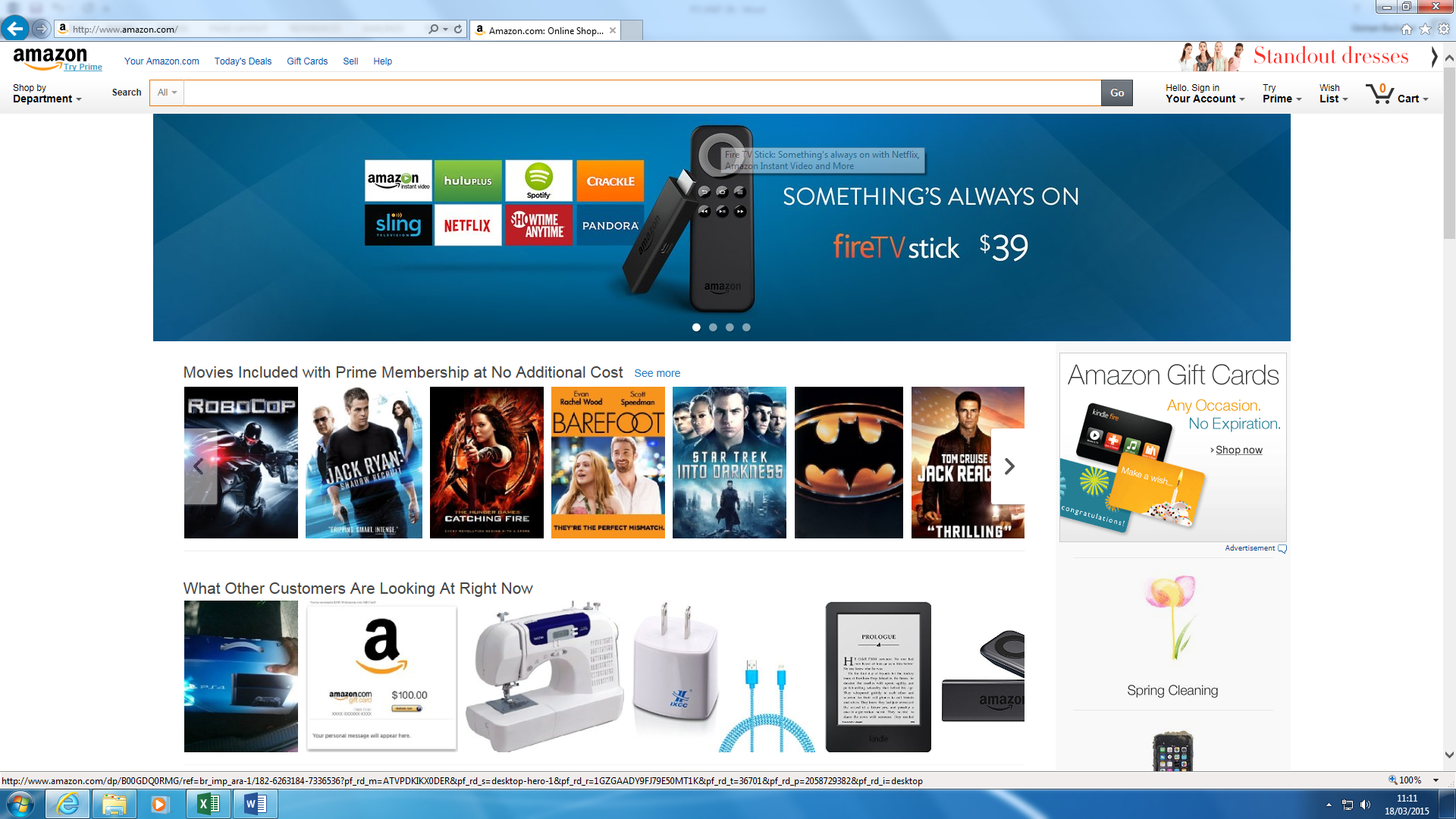
**Introduction**

In this report, I will discuss the security risks that an e-commerce would face. Some of the topics that I will discuss in this report are the following:

* ***Security*:** risks e.g. hacking, viruses, identity theft
* ***Security protection mechanisms*:** firewalls; Secure Socket Layers (SSL); adherence to standards e.g. strong passwords

***Pick a website***

[***www.amazon.co.uk***](http://www.amazon.co.uk)



* ***Explain the risks to the data stored on the website –*** *Hacking, Viruses, Identity theft*

**Hacking**

Hacking is someone who seeks to weakness and gains access to a computer system, or a computer network. Hackers are always doing these unexpected results to gain access to the data. The ways that these attacks could happen is by finding out the identified target, potential ways of these attacks and exploiting the system. To protect the data, you can use secure the system by banning unnecessary and unsafe websites that the user explores, scan the system for any viruses, and they are many other ways to secure the system. The effects it has on the e-commerce websites is that they could break into the website by purchasing, or abusing, any customer information that is not right. They could get information from another person’s account, and they could be purchasing products that the user does not even know about.

**Viruses**

The technology has increased drastically and they are number of issues that the business needs to become aware. Malware is one of the risks that the business needs to solve. Malware is a malicious software that disturbs the network to gain access to private information of any network. Malware is not just a one virus, but it includes a number of issues such as worms, Trojan horses and spyware. To prevent his from happening, of course, each computer needs to have an anti-virus to get rid of these malicious attacks. Malware could be on what the user uses to on websites i.e. the user visits a website full of malware. Once they click on the ‘fake’ advert, the malware can gain access to the account. To resolve this situation, the IT administrator in the business can prevent and block the website from gaining access to the virus account. In addition, having an anti-virus, it could show the user that the website is safe or unsafe.

**Identity theft**

This is when someone uses someone else’s identity to gain access to their personal belongings, or purchase any product in their name. Some types of personal belongings they could use is the following: name, credit card, number, committing crime, and many other. This is used within a website, because some people could get some products from the e-commerce website, without seeing their face, and the original person not knowing about it. This could be a hectic ride for the business, because if the original user finds out that these purchases have been made, he could want a return. This results badly for the business.



* ***Explain the security protection mechanisms* to help reduce the risks** – *Firewall, SSL, HTTPS, and RSA Certificate with Adherence to Standards e.g. strong password.*

**Firewalls**

The benefits of using firewall are that it secures the computer network. It disallows other networks from entering your secured network. As it blocks other networks, it blocks viruses and hackers from entering the network. It acts like a secure “wall”. It does not let anything past it. For organisations that have secure data on their computers, it is vital that they tell/ask all employees to keep their firewalls ON. It is important and if anything is let past, it can access the files and the virus can spread/multiple quickly. The disadvantages of using firewall are that it acts like a central point of attack for intruders; and if they are passed firewall, they have access to the whole network. In addition, it only protects one point of it, it does not protect the other parts of it e.g. modem. The effect of using firewall on e-commerce is that it blocks any unauthorised users gaining access to any information that is not allowed by the user. The effect on an e-commerce website is that it can gain access to all of your information if the firewall has been broken in too. This needs to be looked after too, as well as the computer.

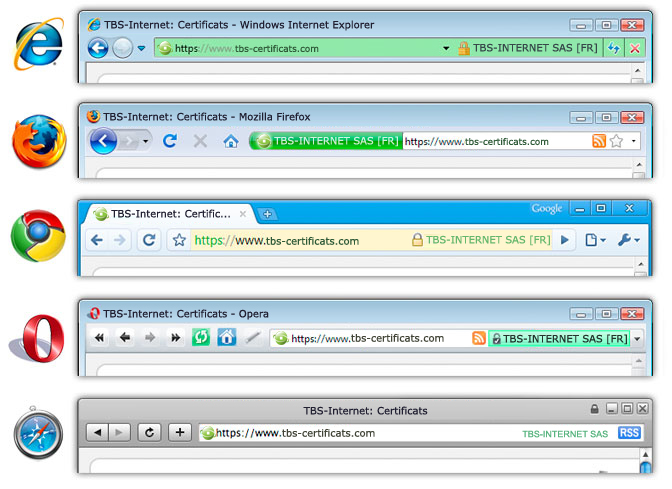
**Password**

Passwords is a set of characters (any on the keyboard) that needs approval to gain access to the users resources. A password for a social networking site is compulsory because you need a password to gain access. A password could be set on many sites and accounts such as:

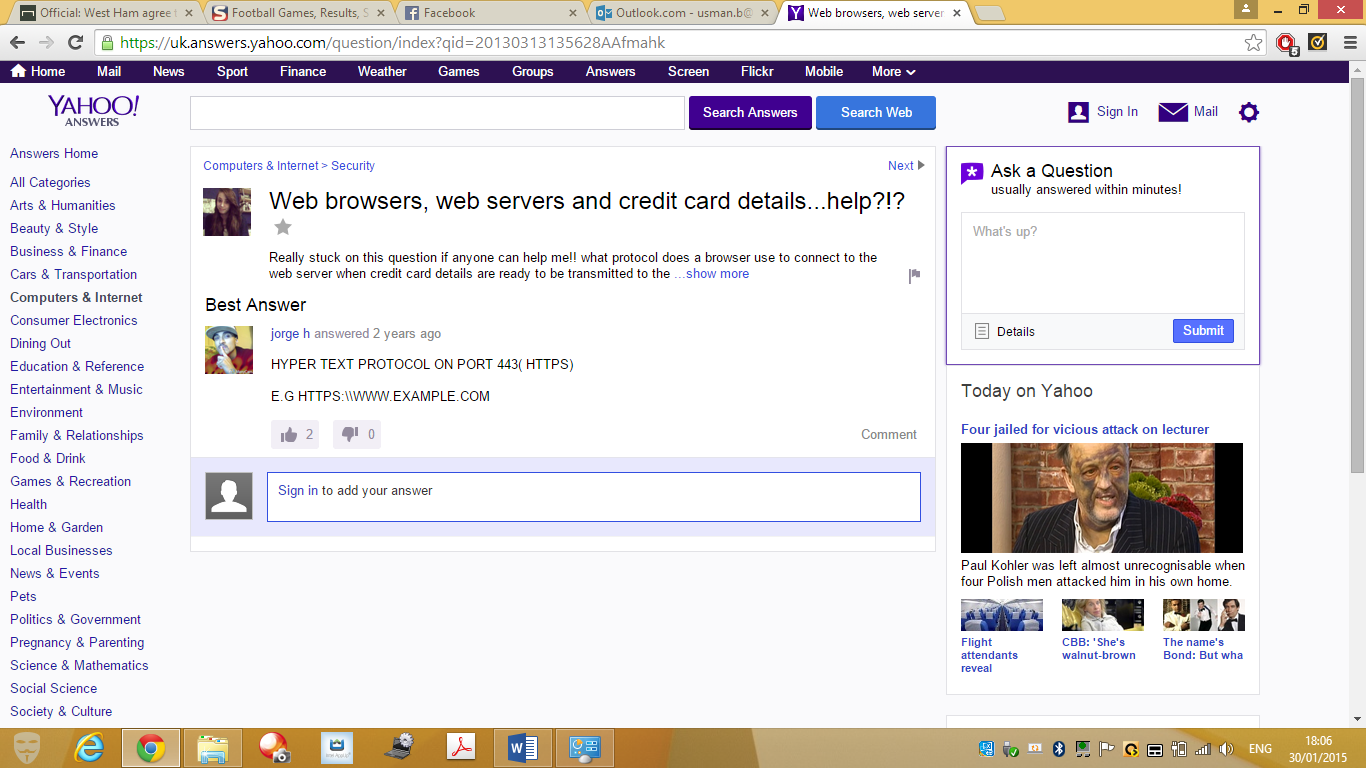
* Users account for a PC
* Any social networking site e.g. Facebook
* Smartphones
* Tablets

The advantages for using a password is that if any other user tries getting access to your account, a password is required. If the user does not know the password, he/she cannot get access to your account. However, if you keep a simple password, it is highly likely that users and hackers may get access to your account and delete the files. Another disadvantage is that you need to remember the password. If you do no not remember the password, you cannot get access to your account. It is advisable that the user keeps a password that he will remember. Customers should use strong passwords to prevent any unauthorised users gaining access to the account. This is crucial for the person, and it is key for them to remember it too. A simple rule the e-commerce website could do is that once they are making the website, they can put a bar on whether the password is strong enough. Therefore, this would warn the customer to make the password stronger. An alert could be sent to them to remind them to use a strong password.

**SSL**

Secure Sockets Layer is main job is to link the server with the client. This means it requests and responses to encrypted data. This is tended to be used in web browsers, or even mail servers (e.g. Outlook). This not only links it between the two, server and client, but secures it too. If the hacker traces down between the links, it can gain access to the information. It uses algorithms, and secures it too. SSL-websites begin with the URL as HTTPS rather than HTTP. Internet Browsers, who understand SSL, are Google Chrome, Internet Explorer and they are many more. It should show the user that the website is trusted by the URL beginning with HTTPS.

**HTTPS**

Hypertext Transfer Protocol (HTTP) is a secure way for information to be travelled. This encrypts data before it has been sent. Accessing information on a website has to go through a herd of security before it can be conducted. As stated before, HTTP is involved by the user going to the URL if it is using HTTPS. This means, that the HTTPs is securing the website. If the user wants to secure the website, it would want more security added on to it. This involves more layers, and encryption added on to it. For example, if any bank details was to be used on the website, HTTPS would be involved and SSL or many other layers to secure the data so that others do not gain access to it.

**RSA Certificates**

RSA is a company in America that uses public key that is widely used to secure data. RSA stands for those who came up with the idea. They are the co-founders of the company Ron **R**iverest, Adi **S**hamir and Leonard **A**dleman. This is linked to e-commerce for the transactions they have made online. Through security, RSC certificate is linked by the encryption using a public key; which uses the SSL for the information to be secured. The process works by the following steps:

* Receiving information
* Decrypting the information by using the public key
* This is called *key pair.* This enables data to be captured without any trace of the user finding out about it; this way it will be unreadable on the journey.

The ‘certificate’ part comes in when each public key is different and needs to be certified. When someone is creating a website and he/she is using a public key that does not belong to him or her. They need to get is certified by this company (RSA). This company helps the user for any problems they face. This could be through security, or anything else the users have issue.

* ***Explain legislation in place to reduce security risks –*** *Data Protection Act 1998, Copyright Legislation, Computer Misuse Act, and Freedom of Information Act.*

**Data Protection Act 1998**

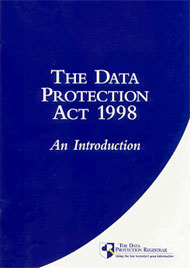
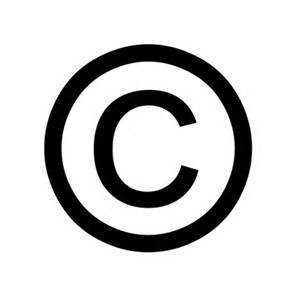
**[](http://www.google.co.uk/url?sa=i&rct=j&q=&esrc=s&frm=1&source=images&cd=&cad=rja&docid=3YCYOuyDvVgVYM&tbnid=-SeqgpgXdHO-wM:&ved=0CAUQjRw&url=http://www.teach-ict.com/gcse_new/legal/dpa/miniweb/&ei=cG9NUt_OG-is7QaA5IHICA&bvm=bv.53537100,d.ZGU&psig=AFQjCNH7WfTRlEOHAMkDpTEvIxgDJZWRUA&ust=1380892906437598)**This act was introduced in the 1998s for businesses or any organisation that deals with information, that transfer data needs to be lawfully processed. This law was set for every employee, as this is vital that the employee’s vital information cannot be reach to anyone. Only certain information is taken, to ensure the safety of the employee is harmless. It is supposed to be secure so nobody can get hold of the information. Data has to be confirmed that the data is accurate. This links to Amazon, because certain employee’s information cannot be held with another functional area/employee. For example, if the human resources department have all the data for the employees and the finance department asks information about details about the employee. They will give the basics; name, how much they get. They cannot give anything else. If the data protection act is misused, they will either be fined, prosecuted. Others can get hold of this vital information and can do anything with it. They will be fined, as they have not followed the legislation that was set. If Amazon were to be in trouble, they will receive a heavy fine. For example, if another business were named Amazon, and this company used it without the other businesses consent, they need to rebrand it or change the name.

Figure 1

**Computer Misuse Act 1990**

This legislation was introduced in the 1990s for businesses, or any organisation that deals with information to treat and not misuse information that they provide. For example, for Amazon, the finance department will deal with PCs, which they will be provided usernames and passwords for the computer. This links to Amazon, because data will need to be secure. If people get access to the data, they might delete it and misuse it. If you get access to the information, it is committing a crime. This will be needed in a business, because if another employee gets hold of a piece of information that is not relevant to their needs, they will be breaking the law. Some examples of misusing information can be hacking to another person’s account or material, computer fraud, physically taking someone’s information without permission. According to the link provided below in the reference, if a person breaks this law they could go to prison up to 12 months/ or obtained a fine. These can be some of the issues depending on how high level of committed crime was committed.

**Copyright Legislation**

Copyright is a legal concept enacted by the government that enables businesses or any owner of a graphical image that give the owner rights and policies of how to use the unique work that they have created. It gives a licence so it can let others use it. This is the copyright logo that could be inserted within the unique granted image. This shows that it has been copyrighted. It is not as big as this but it is small. Many people need to recognise it before use.

**-Copyright free**

[](http://images.tentebranda.org/free-copyright-images/free-copyright-images-7/)Copyright free, as the name suggest, is has no licence over the use of the image. This means that the graphical image can be used on works for free. The major way the image can be copyright free once its licence is expired. For it to be copyright, it needs to be licenced and continued to be reviewed. Once it has not been licenced, it is copyright free.

**E-Commerce Regulations**

Electronic Commerce Regulations (2002) is set for businesses and it includes rights for them. These rights include the following:

* Allowing customers to replace order, if anything is gone wrong. For example, instead of 10, they should have typed in 100.
* The business should provide information about themselves e.g. name, location
* Receipt should be available for the customer
* Communication should be enabled

These rights have to be acknowledged. If anything is wrong with the product, the customer has to have these for an e-commerce website.

**Freedom of Information Act 2000**

This act involves information by public authorities. These could be companies such as NHS, sate schools, police forces and other public sectors. They hold information in two ways. One of the ways is that these public authorities are obliged to publish certain information, and the other way is that the member of public is entitled to request information. This is not entitled straight away. A person cannot demand another person’s personal information just as if they want too. If that same person wants to see information regarding themselves, he or she is entitled to it under the act of Data Protection. This is related to e-commerce, because the web owners can hold information, and the customers are entitled to receiving it. This also means that the owners need to treat all information equally, and disclose any information.

Figure 2