**M2 - Discuss how security issues in e-commerce can be overcome**

**Introduction**

In this report, I will discuss how security issues can be overcome in an e-commerce website. I am going to be discussing about Secure Socket Layers, HTTPS & RSA Certificates and strong passwords.

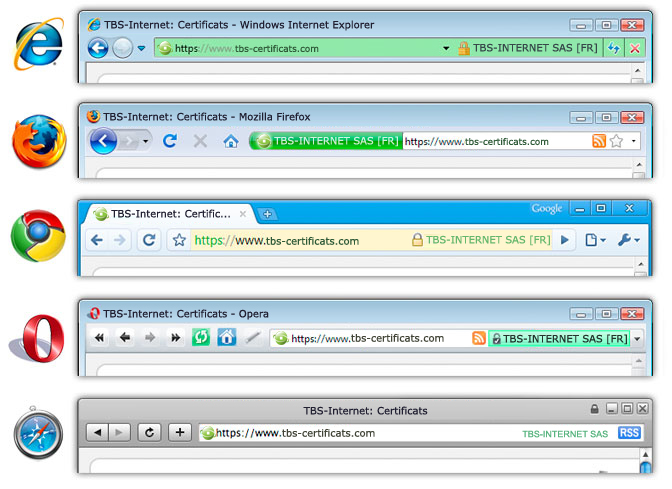
**Password**

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.

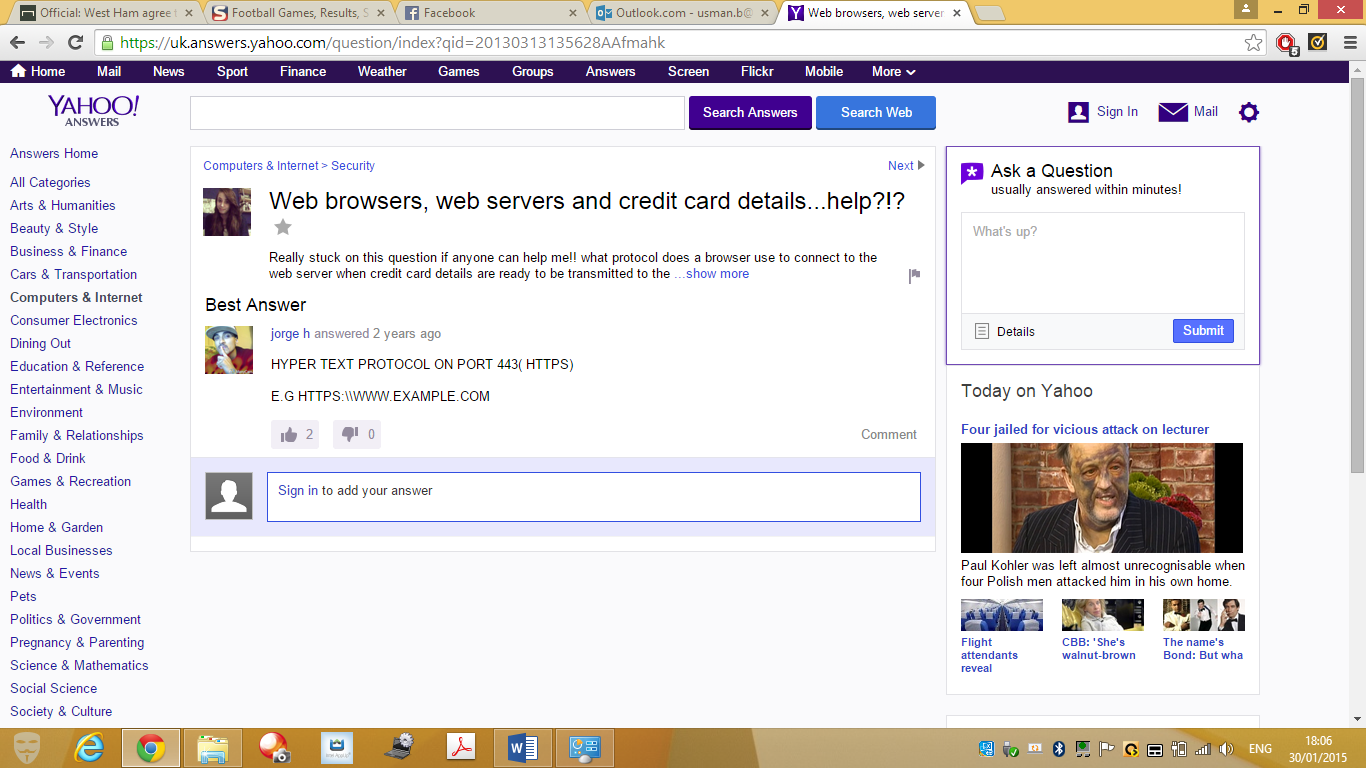
**SSL**

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.

**Encryption**

Encrypting is the process of encoding a message or data so that unauthorised users cannot read it. This means it translates the data into a secret code when it is not possible for the user to read. This is the most effective way of securing data. It is a possibility that it could prevents any hackers from to be able to read the message. The advantage of encrypting is that the user does not need to put extra security on the file(s). It already has encrypted on the file(s). This can save money on getting extra protection. However, the disadvantage of using encryption is that one the encryption is compete; the user can gain what is in the files. In addition, it takes time to crack the encryption.

**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.

**Alternative Authentication Methods**

The four possible other alternative authentication methods are:

* Pin
* Password
* Fingerprints
* Smart Cards

Password is very cheap, and it is very simple. Everyone uses this, and some passwords can be very easy to hack in too. For example, if I named by password my name, and someone who knew my name, got in to my account. This is because it was too easy for the person to get in too. This goes same to pin, but it is not that easy to get in too. Smart Cards are smart, but if someone has gained access to the smart card, then issues could be raised. However, the one with the most security goes to fingerprints. The only way the user can gain access is to use your thumb. In addition, that person needs to be there for the user to gain access to the account. Therefore, this makes it the most security out of all.

**Conclusion**

As discussed, I have learnt that securing your account on a website (especially e-commerce) is important. People can gain access to the account very easily if the customers are not careful with the way they treat it. They are many ways in which we have discussed for the user to secure the account. Hackers could gain access to the ‘simple’ passwords that users can. However, the alternative methods are very secure e.g. Fingerprint.

**Reference**

<http://www.ehow.co.uk/list_7301132_alternative-authentication-methods.html>

<http://cuc.carnet.hr/cuc2005/program/presentations/g6_dukic.pdf>