How security measures in e commerce can be overcome

Prevention of hacking

The issues that all e-commerce sites have to deal with is mainly hacking. If a hacker were to hack Treading Ahead and completely change information, the layout and design, and steal all information from the website, no consumer would want to use their website, and it would therefore be shutdown. In this case, Treading Ahead would need to prevent hacking in order to have secure customer information, and not having them available for hackers to access. If a hacker were to be able to access customer information, many problems can occur such as fraud, identity theft, and stealing money from having access to bank information. To prevent hackers accessing Treading Ahead’s databases and information and data that are to be only seen by certain staff, specialist software would be required to be installed onto the system so that it can be able to check and look at ports that are on a computer and see if they are open or closed. If ports are found open, it’s gives hackers access to the computer system and allows them to view information. For example if Treading Ahead was to leave a port open, and a hacker has the same protocol as Treading Ahead, they can use it to send and transfer data across the network, stealing plenty of information. To prevent this Treading Ahead should make sure that they close all ports so that hackers cannot gain access into their e-commerce website, and not steal information.

Viruses

Viruses occur as a problem for e-commerce websites as it can attach itself onto emails and programs, being able to replicate and cause problems for computer systems and web servers. If a virus were to be planted onto the website and a customer were to visit the website in order to purchase something online, customers would be warned by their search engines not to enter that website, an antivirus would too alert the customer not to enter the website, therefore making the site not trustable. If customers cannot trust the website they will not use it to purchase goods. For Treading Ahead to be able to prevent viruses, they would have to install antivirus software not only to all their business computers, but web servers too. Antivirus software is able to detect and prevent viruses from attacking a computers system, and with that Treading Ahead should update their antivirus every day, keeping out viruses. As new viruses are made and found every day, it is the antivirus’ job to prevent all virus attacks, keeping Treading Ahead’s computer system and web server safe from viruses.

Identity theft

Using an e-commerce website means that a consumer is required to enter their personal details and bank details in order to order and receive their items purchased. Due to being required to enter personal information into these websites, Identity theft has been a problem that occurs when a criminal steals a customers’ details and claims it to be their own, resulting in this being a difficult issue to tackle. It is mainly detected after the victim notices that they have to pay for purchases made online or by card that they have not paid for, and the thief could also use their details to claim money that belongs to the victim. In order to prevent identity theft, it would be ensured that Treading Ahead are to increase the security on their website and make sure that customers change their passwords regularly.

Firewall impact on performance

Firewalls are installed so that it can block out any unwanted access from accessing private networks. It controls exactly what goes in and out, and is to protect a computer and computer network, allowing only authorised accesses to access the data. Firewalls set up gateways which allows only authorised traffic to access the network, and any other traffic that are trying to access the network are to be inspected. If a customer were to go onto the Treading Ahead website and passes through the sites firewall, it will not allow the customer to see the scripts running on the page, preventing viruses and hackers attacking their system.

Secure sockets layer

Websites having an SSL (Secure Sockets Layer) ensures customers that they have a secure communication whilst using the internet. The SSL is a protocol that is made specifically for being able to send information over the internet. Treading Ahead would need to use an SSL on their website as it secures customers when they access their account online or make online payments. Having an SSL provides endpoint authentication, which in this case means that the server and user are to identify who they are; the customer would do so by logging into their online account on Treading Ahead’s website. Treading Ahead would then need to use certificate-based authentication so that unauthorised accesses cannot read data entered into their site.

HTTPS

HyperText Transport Protocol Secure (HTTPS) is the protocol used on many websites on the internet. If Treading Ahead were not to have an HTTPS, data entered into their website may not be protected as it is the HTTPS that protects data entered into websites. It would be best that Treading Ahead have a secure HTTPS so that when a customer enters their bank details into their website it would be protected, by the websites HTTPS. The way in which HTTPS protects data, is that the protocol uses encryption to protect the data, ad so it is ensured that Treading Ahead have an HTTPS to protect a customers’ bank details when entered into their website.

RSA Certificates

RSA certificates are a way of using encryption for security, so that people accessing the website are all identified by a digital certificate, attached with a digital signature. Using an RSA certificate confirms the identity of a sender or recipient. The reason why Treading Ahead would need an RSA certificate in order to overcome security is because it provides security when it comes to customers using their bank cards to purchase products on their site.

Strong passwords

E-commerce systems and web servers are both informed to use strong passwords so that no unauthorised accesses can access them; this is the same for all computer users. Strong passwords must contain both letters and numbers along with capital and lowercase letters, symbols included and should be more than eight characters long. As an e-commerce website draws in many hackers, it is ensured that Treading Ahead create a strong password for both e-commerce website and web server they use. The stronger the password, the less hackers can guess them, making them move on and away from the website.

Alternative authentication methods

A common method of authentication is the use on digital signatures which verifies a user’s identity. It allows a user to be able to authenticate a document over the internet. For example, instead of a customer signing a document in the traditional way by using pen and paper, they can do it online using their digital signature to be able to sign documents. Another method could be the use of passwords. Using usernames and passwords identify a user signing onto a website, and if for instant signing into a banking site, extra security information are used to identify the user even more, and when entered correctly they are able to see their banking information, whereas if incorrect they can not access the website.