E-commerce security

Business, E-Commerce

Any business that operates online Is going to be at risk from Internet threats and because of this the business must ensure to implement security on its network systems. Businesses need to be able to show that they can keep customer information safe and secure, this will reassure potential customers and widen your market potential. Prevention of hacking- E-commerce sites need to be able to prevent hacking so as to keep both business and customer data secure.

If customer data is stolen from a business's database then It Is possible for the thieves to steal those customers' Identity, this Is known as identity theft. Identity theft involves a thief stealing the personal details of someone and using this information to apply for services such as credit cards, loans and mortgages whilst pretending to be the person that they have stolen the details of, and it can be difficult for this crime to be detected If the thief has a large amount of the person's details and is often only discovered when the victim receives correspondence requesting payment for the thief's spending.

The type of personal details that e- commerce sites keep about their customers provides enough information to commit Identity theft so It's Important that all e-commerce businesses protect their customers' data. Firewall- A way to protect customer information Is to have a firewall on the business's database. A firewall builds a protective virtual barrier around the network which only allows authorized programs access to data.

When a user views a web site that has passed through a firewall they may not be able to see all the features of the site, this Is because the security policies on the firewall can be set to block certain types of script's running on

the user's computer. This is done to prevent viruses and hackers from attacking the system. Authentication- The most common but also effective ways of using authentication to protect your network is to ensure that all users have strong passwords.

A strong password should have both: letters and numbers, capitals and lowercase, symbols Like %$E and should be at least 8 characters long. Hackers can take advantage of any weak passwords used by users of a network, because of this passwords should not be personal to the seer, for example their dogs name as this will be easy for a hacker to find out.

Software programs known as password breakers can be run to check every available password possible by changing a variable each time, e. G. It will start with O then 00 then move onto more until it changes to making one of them a 1 and so on until it 1 password, the longer it will take for the password breaker to get it correct, which is risky for them as they can be detected by security programs so the hacker will normally give up if it takes too long.