How to manage risks

Cyber crime

As IT developments increase, and the more the internet is being used, this brings in more risks of cyber crime. For example the case of fraud over the internet has been an issue as customers’ credit card details are stolen, even as the chip and pin was introduced to increase of security of buying by using debit and credit cards. There is a downside to e-commerce which is when illegal purchases are made from unnecessary websites and dodgy organisations which can offer illegal merchandise to the public and adult products to underage consumers. This can be pretty uneasy for police to recognise the issue.

Diverting financial assets

Criminals can be able to transfer large amounts of money (megabyte money) across the internet in a way that is quick and easy. Although this is illegal, the process is made easier because of the fact that plenty of online buyers are making transactions, buying products online with their debit and credit cards and so it is quite tough to identify and trace individual transactions on a global scale.

Sabotage of communications

Sabotaging of communications systems mostly happens through viruses, which could even be sent as for example email attachments. Software bugs can also be a threat but although they can be non-malicious, the attack is most likely to be a risk to software or a system as a virus attack. Bug usually occurs when software is introduced early onto the market with inadequate testing. In order to protect our technological services against viruses, security software (such as Norton or MacAfee) is required to be installed onto home and work computers.

Intellectual property theft

Organisations have special privileges to a design of their product which they have patented. Patented products can’t be copied by anyone outside of the organisation. A lot of creative work and products by an organisation are not patented, but are kept under security by copyright law, for example paintings, images, literary articles such as novels and poems. The owner of the patent or copyright to a product has the privilege to make or reproduce the product and no one else can do this without permission. If an organisation were to copy or use a patented or copyright material without the owners permission this is called stealing intellectual property. A lot of people tend to copy and paste information from the internet and use it ask their own work, not knowing that it is illegal and seen as an act of plagiarism.

Denial of service attacks

Denial of service attacks are caused by hackers that effect networks on computer systems. Deliberate attacks and non-malicious attacks can occur, such as interruption to the operation of a network. Denial of service happens when a hacker floods a server with requests, attacking websites and causing jams. Large websites like Google or Twitter have security systems to prevent denial of service attacks and to keep their websites safe and protected. Firewalls are set up to deny DOS attacks.

Preventive technologies

Preventive technologies support the management of hazards. Preventive procedures consist of systems that monitor compliance with data protection and firewall software that can try to stop admission to certain websites that are undesirable.

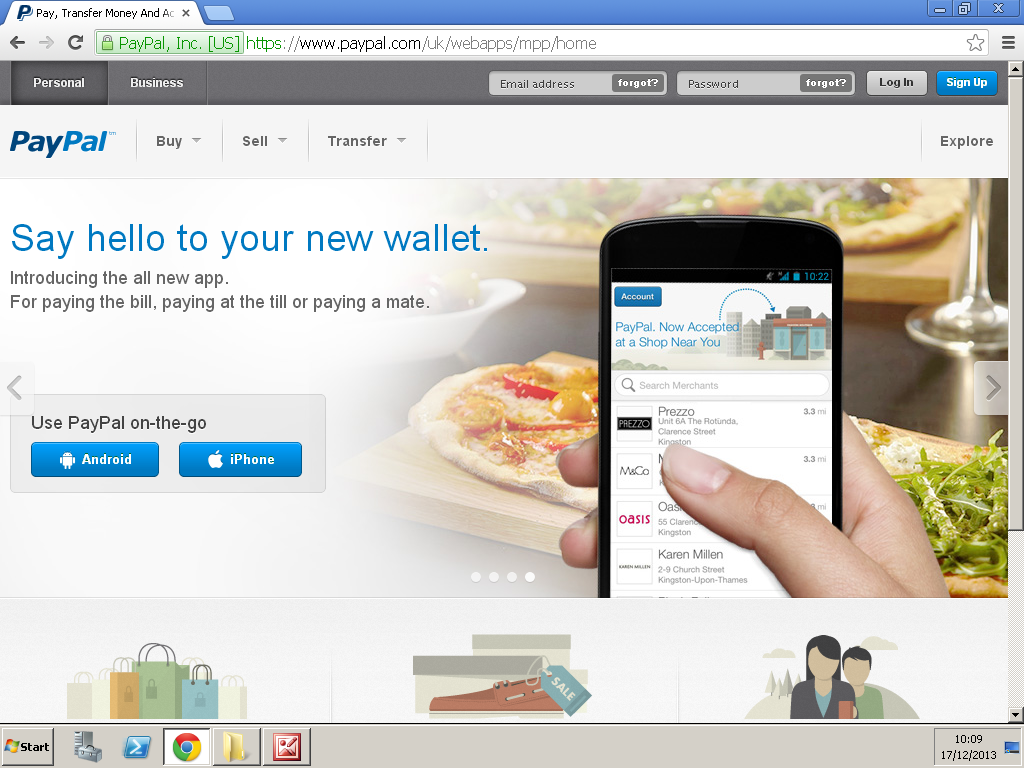
Firewalls

A firewall is software designed to protect computer systems from unauthorised access from the internet that try to access private networks. This improves a computer systems level of security. Firewalls tend to use filters to block unauthorised material and potentially dangerous attacks such as viruses from entering the system. Firewalls can be either hard ware or software that limits access to networks. Routers that pass information between networks also contain firewall components.

Access control methods

As lots of people use the internet, wireless connections are needed to be protected due to unwanted users obtaining access, and so they have to be security-enabled by having passwords for access. If wireless connections remain unsecured, any unauthorised users are able to connect themselves to that wireless connection; they can also access private information as well as email accounts and bank details. Phishing is a main problem that people face from criminals. It can be carried out by the use of spam emails claiming to be from a specific bank that a user is subscribed to. Emails like these try to trick people that they have to check their bank account due to security errors and so users would click the links provided, sign into their account and have their bank details stolen for criminals to be able to access it and be able to withdraw funds. Nowadays banks give out warnings not to respond to these emails and to report them.

Secure payment systems

Websites such as PayPal that are used for making payments online should be accessed if fully trusted. When using websites like PayPal users would have to make sure of the signs that assure them that the website is safe. 

For example when going onto the paypal website it fully assures users that the website is safe, as you can see above that it has a padlock with ‘PayPal, Inc’ written next to it to confirm that the website is safe. Paypal also offers VeriSign Identity Protectin Network (VIP) as an supplementary layer of security when signing into the website.

Disaster recovery

Organisations need to have plans in order to ensure that information they have stored electronically is protected and backed up. When it comes to files like financials accounts, it is recommended that they should be backed up regularly. As for individuals backing up files and restoring deleted files can be an easy process as they are able to save files on storage devices like a USB, but for organisations disaster recovery plans are needed. For example an organisation needs to have a solid plan if files are needed to be restored or if they are accidentally overwritten or even become corrupt. Each organisation should have a system for backing up everything on the system and should make sure that backups are not kept on the premises.

|  |  |  |
| --- | --- | --- |
| **Risks** |  | **Preventive technologies** |
| Cyber crime |  | Firewalls  Firewalls are set up to deny DOS attacks and to act as a barrier between your computer’s networks from destructive elements. Firewalls also protect important information e.g. bank information from cyber crime as well as diverting financial assets. |
| Diverting financial assets |  | Secure payment systems  Cyber crime can be stopped by having secure payment systems so that (for example) hackers can’t access bank your bank details online, and so extra protection is added to prevent this |
| Sabotage of communications |  | Access control methods  Protecting users who use wireless connections to view bank details online and can prevent criminals from getting into peoples bank accounts and stealing money |
| Intellectual property theft |  | Disaster recovery  Disaster recovery would also help sabotage of communications as it requires a backup. If users backup their files and data they can use backups to restore all their work and information. |
| Denial of service attacks |