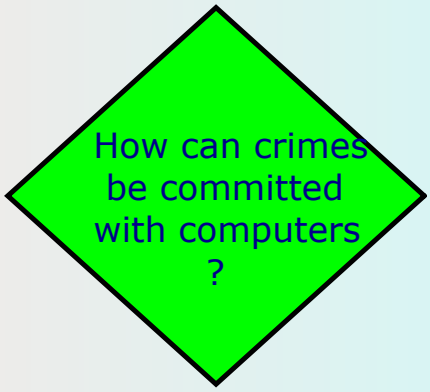
E-consumer Awareness

Security



Which are directly related to e-commerce?

Task

- Who holds information about you?
  - List all the organisations and people.
  - What information do they hold?
  - Why do they hold it?
  - What other purposes could it be used for?

Visit www.amazon.co.uk

If you signed in, what information would they hold about you?

Look at your website and make a list of the details they would keep about you.

What information is held about you?

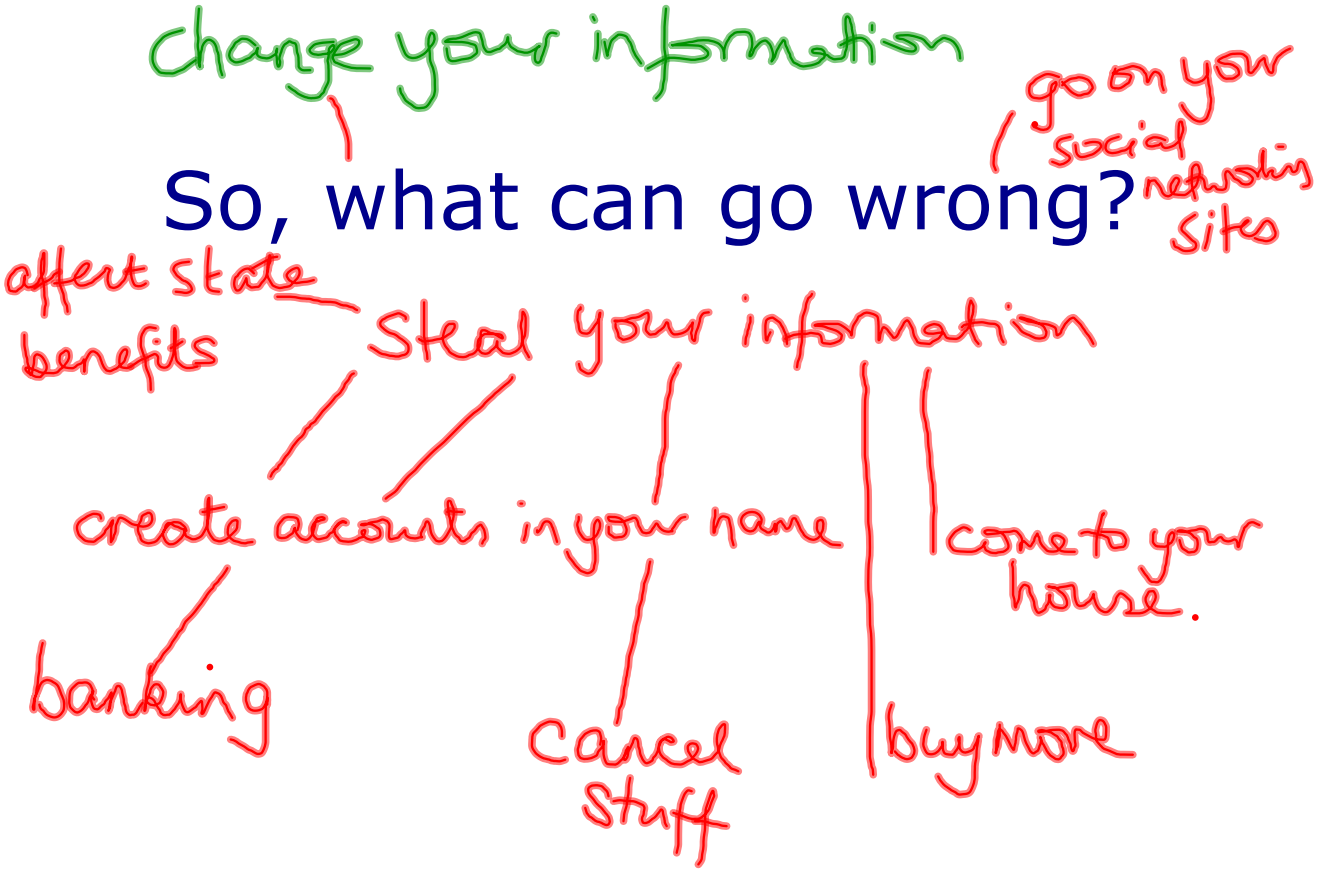
- In any business transaction a business needs to have some information about the customer… what they want, colour preference, size etc.
- Additionally they may wish to gain information to be used in marketing strategies and developing its product range.
- A significant amount of this information is provided by the customer and some is gained by transactions or via a 3rd party as discussed previously.

from business to business. E.g. direct debit information, your car make model etc for car insurance.

- Most of this information is relevant and necessary for the transaction to take place.
- Think about what is held about you by school is it necessary.

that is held is not directly relevant to a specific product it allows the business to market goods that we may be interested in.

- As consumers we have 2 main issues:
  - we don't want other people to know all of our information such as our credit rating
  - we don't want the information to be wrong!


change your information
go on your social networking sites
So, what can go wrong?
affect state benefits
steal your information
create accounts
in your name
banking
cancel stuff
buy more
come to your house.

How accurate is the information

- Getting bills when you have already paid them, getting bills for people that are deceased, getting court summons for repayment of a car you don't own….
- Human Error is normally a major factor in this and the use of automated systems has generally dealt with a lot of this but has brought its own range of problems.. Most of which are due to the original source data being inputted!

How accurate is the information

- Verification- double checking the input of data!
- Validation – settings adjusted on a computer that only allows certain characters to be entered.
- Up-to-date information – information should be updated regularly to remain accurate and customers can help with this online. Frequently customers are asked to check their details during a transaction to check they are still up-to-date.

What is the information being used for?

- People are becoming increasingly concerned what there data is used for.
- Data is passed easily between companies, indeed the electoral register is in the public domain.
- People are becoming more and more annoyed by cold calling and now cold emailing.
- This is not an issue that will go away, with identity cards becoming ever more likely the amount of information that is held on is ever increasing.

Who has access to the information?

- Much of the data is public but there are other banks of collected data that are stored on us:
- Data that is sold to others
  - Many companies pass data to other companies, illegal without permission but most people tick the agreement box unwittingly (or fail to tick it!). This information can be sold to other companies to help them market their goods.

Who has access to the information?

- Collecting email addresses
  - Email addresses can be given freely as a way to log into a site. They can also be detected by cookies or a form of spy ware. Random trial and error also occurs with well known domain names. e.g. hotmail.com
- Credit card details
  - We use the internet and the phone to conduct credit card transactions. This has lead to a wide spread fraud. Whilst there are still traditional approached to gaining cards e.g. robbery there are now much more sophisticated ways of gaining the information:
    - Searching a hard disk
    - Searching rubbish for letters
    - Spy ware
    - Receipts form cards

- Old PCs
- Spyware and trojan horses

Giving away your identity

Example from N Ireland

What are the main potential threats associated with ecommerce?

Describe the different methods used to carry out these threats.

to help:
white book ch 2.6

Write notes for Thurs.

How is data at risk?

- Phishing
- Fraud
- Hacking
- Human error
- Physical threats such as fire
- Identity Theft

Identity Theft

- The worst case scenario is identity theft which is one of the fastest growing crimes.
- It is incredibly easy to gain all the basic details on a person which can then be used to get credit cards etc.
- Internet banking have had to get a lot wiser over the past couple of years to stop a whole manner of scams affecting there customers.

How can businesses help protect their customers data?

1. Legislation

p64,65
p213

Data Protection Act 1984?

2. Physical protection

Back ups — in a server room-locked
p168,9
very few keyholders.
regularly
not on internet
Responsible staff.
Passwords user ids
Destroy harddrives

3. Cyber security

p169-172

Encryption
SET

The Law: Data Protection Act

- The data protection act struggles to help consumers in this hi-tech society.
- It stipulates that information must be:
  - Secure from unauthorised access
  - Accurate and up-to-date
  - Kept for no longer than necessary
  - Used for the purpose it was gathered
- A lot of theses rules are open to interpretation not helped by our willingness/ ignorance to allow businesses to use our data in a number of different ways.

Security measures

- Aside from legislation there are other ways to protect ourselves
  - Physical Security
  - User ID's
  - Firewalls
  - Encryption
  - SET

Physical security

- Stopping unauthorised personnel getting to the information in the first place may be one way of preventing fraud.
  - Equipping premises with alarm systems
  - Keeping computers out of public view.
  - Locating a server in a room with essential personnel only
  - Storing back-up tapes away from the server

Physical security

- Training on:
  - Use of Bluetooth/ infrared/WiFi
  - Portability of laptops etc can cause an issue.
  - Use of USB's etc.

User ID's

- For both external and internal security passwords and user ID's should be used.
- Different levels of passwords can be distributed allowing levels of access.
- This is valid for home use as well, user id's and logins to secure payment sites are important.
- Not using obvious logins and passwords and having a series of entrance codes is a good idea.

Task

- Read and complete the discussion task on page 218.

Firewalls

- Use to control access to networks.
- They enforces a control policy as to who is allowed access.
- Many people wish to hack into systems and steal there data, it is important companies protect themselves and their clients.
- Most firewall are set to protect against log ins form outside the company.
- Users with in the network can still access the outside freely.
- However Firewalls don't offer any protection form within.
- Firewalls should be part of the overall security system.

Encryption

- Encryption is the scrambling of data normally that is sensitive and confidential.
- Once scrambled it can only be unscrambled by a a computer with the correct software.
- Frequently used for payment transaction on the internet.

SET

- Secure electronic transactions.
- A net protocol developed by Visa and MasterCard.
- It is designed to ensure the security of transactions over the internet.
- SET encrypts the data so it can not be read by a third party.

The management is responsible for ensuring:

- all data handling is legal (DPA)
- risk assessments are carried out regularly concerning the website's security and that of the data
- staff are trained thoroughly and the input of data is checked for accuracy
- staff are trustworthy

don't run off with data
don't divulge data to others.

How can customers help to keep their data secure?

-ensure the padlock (or https) is on your screen before entering details.

- use passwords that are difficult to decipher

- change passwords regularly

- tick the box that disallows the company from passing details to a third party

- dispose of old PCs wisely

- check data is up to date and accurate

- choose reputable websites.

Assessment

- Write a report which identifies and explains
  - Potential threats to customers data collected by organizations via their websites
  - Protective measures used by organizations to protect customer data
  - Examples of relevant legislation passed to protect customer data and how effective it is.
  - Conclusion- This is an overall risk assessment for the consumer- is it worth it or not?

Assessment

- The report should be no less than 1000 words.
- It should be written in word and converted to PDF.
- The work should be attached to your e-portfolio.

information & communication technology

for edexcel applied AS level single award

Description of potential threats

- Part C
- Potential threats to customers data
- Protective measures used by organisations to protect customer data
- Laws passed to protect customer data
- Description of each law
- Effectiveness of each law
- Conclusion- risk assessment

completed by 13th Sep

Security issues for e-commerce

Why does a company keep information about their customers?
What kinds of information might be held about a customer?
What are the potential problems for the customer? (last weeks homework)
How can the company help protect the privacy of the customer?
How can the customer help protect against the threats?
What has the government done to help?
Is it worth it? Write a paragraph weighing up the pros and cons of data protection within e-commerce.

29 September 2010 Last updated at 13:53

BT embroiled in ACS:Law porn list breach

26 August 2010 Last updated at 12:28

Stolen laptop held customer data, admits Yorkshire

3 June 2010 Last updated at 18:21

Lampeter practice 'breached' Data Protection Act
A memory stick (generic) The data was stored on a memory stick

A medical practice which lost the details of 8,000 patients, including their names and addresses, beached the Data Protection Act, says a watchdog.

Last Updated: Friday, 7 December 2007, 10:56 GMT

DVLA 'breached' data protection
DVLA, Swansea
The DVLA at Swansea is conducting an investigation
The Driver and Vehicle Licensing Agency (DVLA) broke data protection rules when confidential documents were sent to the wrong motorists, it has been claimed.

The agency sent 1,215 questionnaires, including dates of birth and motoring offence records, and about 100 went to the wrong addresses.