Chapter 4 - Dealing with organisations you give data to.

In the last chapter Dilbert showed us how to shop safely on-line. However, there is more to staying safe in a digital world than using your browser correctly. You need to be discerning about who you give your data to.

Clearly, It makes sense to deal with companies and organisations that are going to protect your payments and your personal details. How do you tell ?

Well it's a good start to look for evidence of security, Care and Robustness. Some indications exist to help you avoid companies where they have eliminated the security department as Wally suggests

Nobody is really that bothered about their personal data - if someone loses a fiver, they'll turn their house upside down to find it. But lose a CD with a copy of their CV and a copy of their birth certificate and they'll only raise a concerned eye brow.!!!!!

Nobody, consequently, really values the security department in a company – for the same reason. Data isn't hard cash. Wally (above) has just refurbished his den by exploiting this fact. And because nobody thinks they do something important, the budgets the security department get to protect your data aren't very big. With low salary budgets the staff these departments are usually unattractively, boring, sad, ineffective … And, therefore, unlikely to change this prevalent image of themselves.

AND THAT'S WHY YOUR DATA FALLS IN THE WRONG HANDS AND YOU FALL VICTIM TO ID FRAUD – IT'S ALL YOUR OWN FAULT. YOU SIMPLY DON'T CARE ENOUGH,

And what's more it may be too late to do anything about it – if your data's out there, you're doomed. You've banged on for years about civil liberties and political correctness, overly worried about other things, whilst you've been giving data to companies that hand it out to anyone that asks.

Yes there are some rules - people and companies have to pay lip service to some laws but they are hardly policed.

The LAW – Data Protection Act

Although this section is very boring - read it, it is useful. The Data Protection Act was passed in 1998 and came into force on 1 March 2000. It implements in UK law what the loonies in Brussels Euro Parliament call the European Directive on data protection (95/46/EC). It is this implementation of the European directive (equivalents in other contries in europe) that provides you protection.

It only covers the use of personal data (i.e. data relating to identifiable living individuals), rather than companies, pets or dead-people and includes data recorded on both manual records and computers. The law gives individuals (data subjects) certain rights over the way that their "personal data" is processed.

These are set-out in a set of eight principles for the fair and secure handling of personal data that the person holding the data must comply with. These are:

1. **F**airly and lawfully processed.
2. Processed for limited purposes and not processed in any manner incompatible with those purposes.
3. **A**dequate, **R**elevant and not excessive.
4. **A**ccurate.
5. Not kept for longer than is necessary.
6. Processed in accordance with the Data Subject's **R**ights.
7. Kept **S**ecure.
8. Not **T**ransferred to countries without adequate protection for the information.

This can be shortened to **FARSTAR:**

- F – Fair
- A – Accurate
- R – Relevant
- S – Secure
- T – Transferable
- A – Adequate
- R - Rights

Common breaches

Even though I have tried to explain it simply, like most laws, it is extremely confusing. Here are some common breaches:

- You give your details to a UK organisation and they send it to there Head Office in Elbonia- Managers often ignore security to save cost. This would be an inappropriate transfer to company with lower / different data security processes.

- You enter personal details into a website to buy a health insurance policy and this includes the fact that you may be short-sited and are over-weight. Ten weeks later you receive a flood of sales cold-calls offering glasses or weight-loss pills because the organisation has used your personal details to target their marketing. This is a breach of the "relevant" purpose principle – the data was not collected for this purpose.
- You take part in a Drugs trial and suddenly find your name published on the internet – This is often called a data leak and would be a breach of the security principle. Here are some other recent "data leakages".

Brown and Blair's DATA LOSS SCHEDULE

February 2007 - Nationwide Building Society was fined £980,000 by the Financial Services Authority (FSA) for information security lapses. The fine follows the theft of a computer containing confidential customer data from an employee's home.

March 2007 -The Information Commissioner named and shamed 11 TOP financial institutions for committing 'unacceptable' breaches of the Data Protection Act. Customer account details were left in waste bins, skips and bin bags outside branches all across the country.

Oct 2007 - A laptop containing details of bank customers was stolen after a member of HM Revenue and Customs (HMRC) left it in the boot of his car. The computer contained records from finance houses revealing the identity of high value customers who had invested in Individual Savings Accounts, according to research by the BBC.

Nov 2007 - Nearly 15,000 Standard Life customers have been warned that they could face ID theft after a courier's blunder exposed their banking and pension details. HM Revenue and Customs (HMRC) hired a courier to carry the data, which pertains to people who had opted out of state pensions, but the data was lost.

Nov 2007 - The head of HM Revenue and Customs (HMRC) has resigned after it was revealed in parliament that the personal details of 25 million Britons had been "lost in the post". The Chancellor of the Exchequer stated that two CDs with the details of 25 million families had been sent to the National Audit Office by courier firm TNT but failed to arrive. The disks contained names, addresses, dates of birth, child benefit numbers, National Insurance numbers and bank or building society account details.

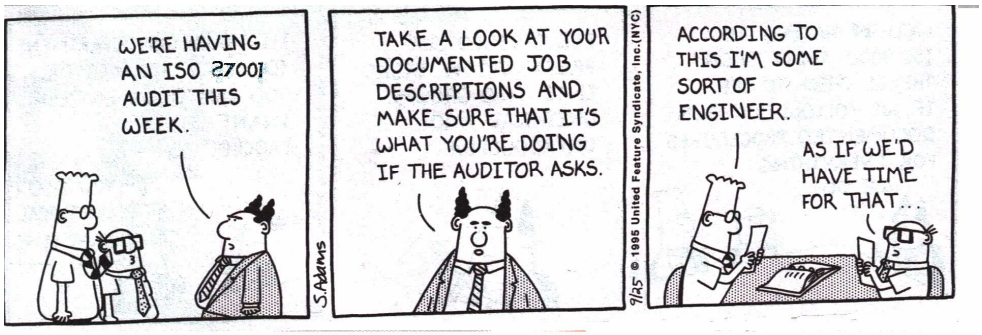
January 2008 - the NHS has lost 5,123 patient records when a laptop was stolen. The information on patients with a blood disorders was contained on a laptop that was stolen from Russells Hall Hospital in Dudley, West Midlands.

If you believe that your personal data is being used inappropriately, distributed inappropriately or kept in an inappropriate manner, you can make a complaint to the information commissioner. Not surprisingly, poor guardianship of salary data (like the POINTEE HAIRED ONE below) is often a cause of complaint.

You also can make a DPA request to any organisation to see all data held about you, if you believe some of it is inaccurate or being held past its reason for collection. You need to put your request in writing, making it clear you are asking for the information under the Data Protection Act 1998) and send it (by letter, fax or email) to the organisation that you are concerned about. They have 40 calendar days to respond to your request. The organisation can ask you to pay a fee of up to £10.00 for each request made – which is likely to cost more to process than the £10.00 you give them. It fact many E-trouble makers make such requests to cause nuisance.

BS7799/ISO27001 - They care more about security

BS7799/ ISO27001 is considered by most authorities in Europe to be the major information security standard. It is just like ISO9001 but for security.



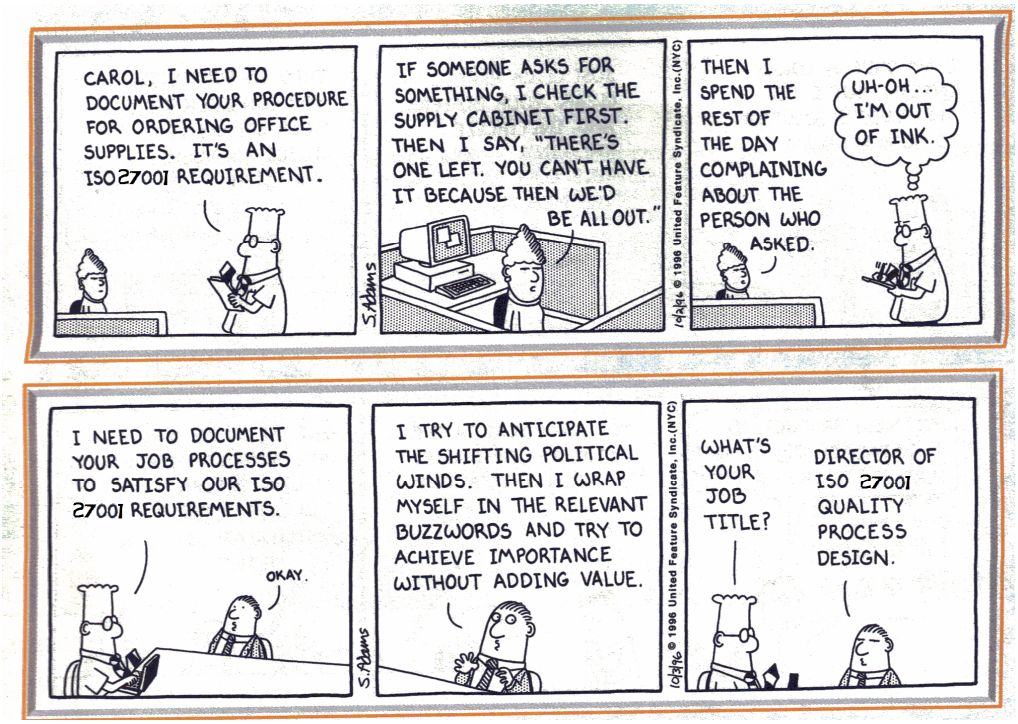
The standard forces companies to evaluate their data security risk and implement procedures/control to protect against these risks. The key controls are as follows:

- Information security policy document
- Allocation of information security responsibilities
- Information security education and training
- Reporting of security incidents
- Virus controls
- Business continuity planning process
- Control of proprietary software copying
- Safeguarding of organisational records

- Data protection
- Compliance with security policy

This process is audited twice yearly and if your company has done a good enough job, you get a badge and certificate.

Attaining ISO27001 is arduous and does specifically compel a company to make sure that their employees understand the importance of security, and specifically data protection regulation.



The fact company has bothered to go to the time and expense of the audit speaks volumes. When dealing with one, your data should be much safer!!!!

ISO27001 is a process focussed certification. The example processes it recommends tends to ensure that reference's for new employee are taken up. However it does not insist on a CV with photo which would thwart Alice's Identity Fraud above – if you are going to bother to take references do at least ensure that the person the referee is talking about is the same person that you will employee by using a CV.

Also as ISO27001 is process focussed, it is possible that an organisation passes it audit and has excellent processes, yet has really insecure firewalls, databases and Webservers. So there are other badges you should look for.

Badges that test technical bits

There are badges that you get for having your Technical bits tested. Here are some to look out for

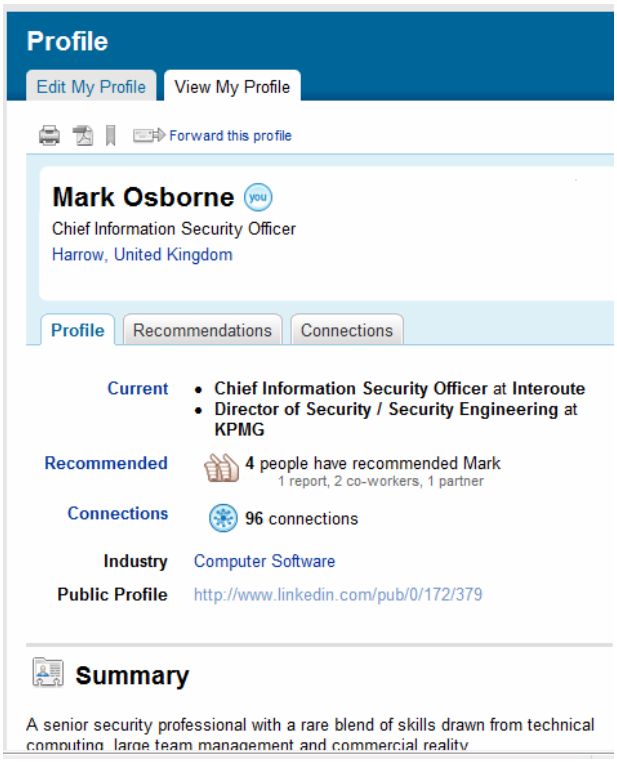
Most of these involve having a “tame hacker” or “ Penetration tester” take a bang at the target website to look for real holes. Choose a site with these badges if you can .

Inviting ID Theft – social network sites

All identity theft is facilitated by the BadGuys finding key details about you – your birthday, your national insurance number, your employment history and other details that would allow them to represent themselves as you.

Social networking sites make it easy for the bad guys – limit the details you broadcast to masses from them – otherwise you will become a victim.

From a site such as Linked-in you can often get a list of contacts and a full career history

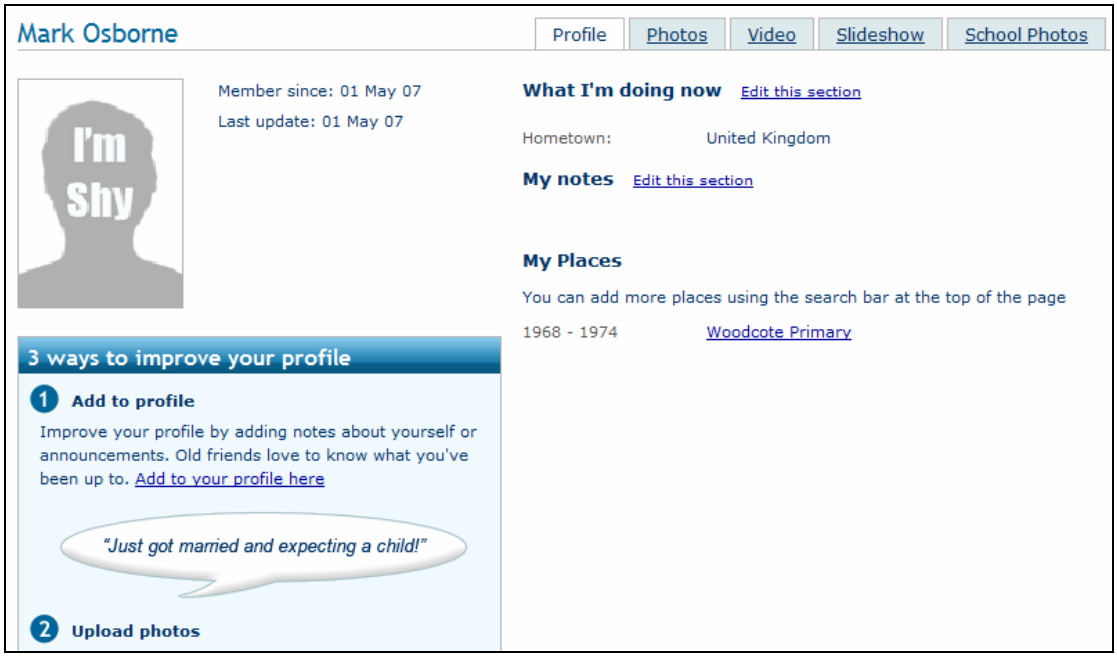


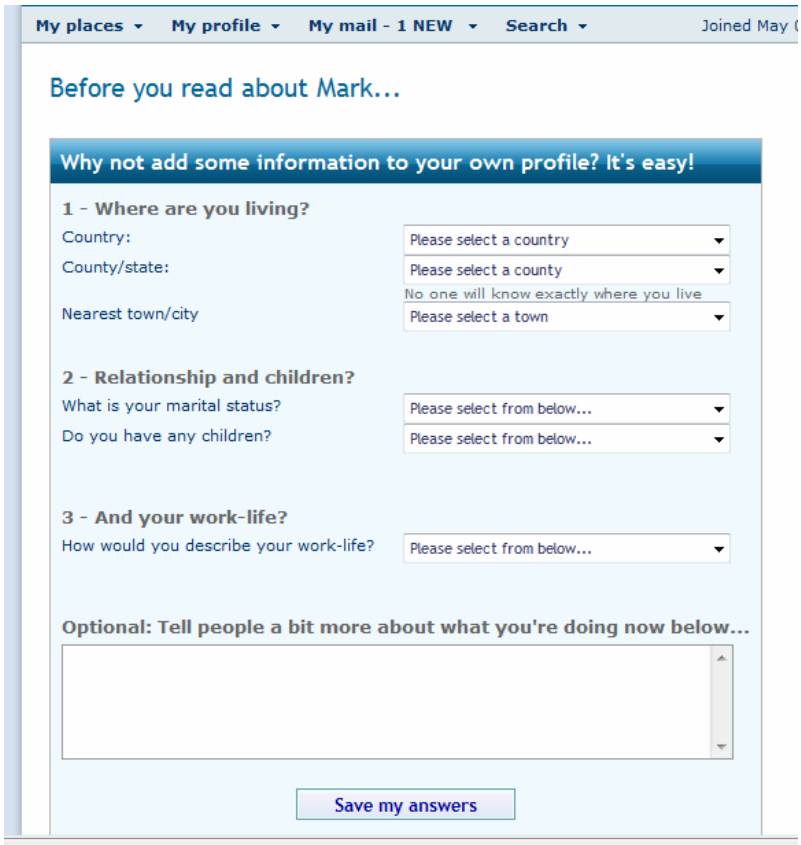
And this is when the profile is set up conservatively, the next screen shows just how much information you can give out if you go crazy-mad ‘n send caution to the wind .

You should be cautious with all social networking sites. This includes

- Linkedin
- Friend united
- MySpace
- You Tube

From these a bad guy can collect a convincing background, home address and even a photo to generate false ids.





Don't use them – if you have to use them, give minimal information.

----------end of chapter ----------