



Literature Review on Internet Crime
for
National Audit Office

Professor Peter Sommer

March 2009

Literature Review on Internet Crime

This Literature Review was commissioned by the National Audit Office in February 2009 and completed in March 2009. Its purpose was to support NAO's review of UK Government initiatives in reducing the impact of such crimes.

Professor Peter Sommer is a Visiting Professor in the Information Systems and Innovation Group of the Department of Management at the London School of Economics and Political Science. He is also a Visiting Reader, Faculty of Mathematics, Computing and Technology, at the Open University.

In a first phase on 10 February 2009 Professor Peter Sommer facilitated a workshop at NAO offices to assist NAO staff in establishing the scope of their project, to identify a range of definitional problems and to determine the precise remit of the existing statistical, qualitative and background research they wished him to cover.

After the workshop Professor Sommer provided a suggested remit in terms of the key questions driving the Review, the basic information needed, the main sources and an outline structure. After some discussion agreement was reached

This Review is the product.

March 2009

1	Introduction to 'internet crime'	9
1.1.	Definitional problems	9
1.2.	Scope of "Internet Crime"	11
1.3.	Scope of this Study	13
1.4.	How "Internet Crime" is dealt with in substantive laws	15
1.4.1.	Fraud Act 2006	15
1.4.2.	Computer Misuse, Malware, Hacking	23
1.4.3.	Harassment, Cyber-Stalking	23
1.4.4.	Disturbing and Illegal Material	24
1.4.5.	"Grooming" of children for sexual purposes	26
1.4.6.	Exploitation of Children in a retail Internet situation	27
1.4.7.	Spam Distribution	28
1.4.8.	DataTheft	29
1.4.9.	DoS, DDoS, Botnets, Extortion	31
2	Research Sources	34
2.1.	Statistics: Quantitative Research	34
2.1.1.	Statistics on General Internet Usage and Growth	35
2.1.2.	Statistics on the use of the Internet by Children	39
2.1.3.	Statistics about use of Internet by older-consumers	44
2.1.4.	Statistics on Social Networking	45
2.1.5.	Crime Statistics	46
2.1.6.	Business Orientated Statistics	58
2.1.7.	Statistics about Cyber-Stalking	65
2.1.8.	Statistics about Sex Offenders	65
2.1.9.	Statistics about Obscene Publications	66
2.1.10.	Statistics about the incidence of malware and spam	66

2.1.11.	Other Reports	71
2.2.	Qualitative and Analytic Research.....	73
2.2.1.	Studies on Internet and Computer Crime.....	73
2.2.2.	Studies about Children Online	78
2.2.3.	Exploitation of children in a retail Internet situation	92
2.2.4.	Miscellaneous Further Articles worth noting	94
3	Review of ‘counter-measures’	96
3.1.	Technical preventative measures that can be applied by potential victims	96
3.1.1.	Patching and updating software and applications	96
3.1.2.	Anti-virus, anti-trojan, anti-malware software.....	96
3.1.3.	Firewalls.....	96
3.1.4.	Anti-spam services.....	97
3.1.5.	Anti-phishing services	97
3.1.6.	Subscription-based external malware, firewall and intrusion detection services	97
3.1.7.	Content Filtering Programs.....	98
3.1.8.	Web-labelling schemes	99
3.2.	Technical preventative measures that can be applied by ISPs.....	99
3.2.1.	AntiSpam	99
3.2.2.	Content Filtering	99
3.3.	NGO-provided facilities	100
3.3.1.	Hotlines	100
3.3.2.	Age Verification Services	100
3.3.3.	Phishing Emails	101
3.4.	Awareness and Educational Programs	101
3.4.1.	General.....	101
3.4.2.	Advice for Children	102

3.4.3.	Advice for “Silver Surfers”.....	104
3.4.4.	Fraud Advice.....	104
3.4.5.	Business Advice.....	105
3.4.6.	Advice from Police	105
3.4.7.	Advice from ISPs.....	106
3.4.8.	Advice from Central and Local Government.....	107
3.4.9.	Instant Response Services.....	108
3.5.	International Research Initiatives	109
4	Conclusions	110

1 Introduction to 'internet crime'

1.1. Definitional problems

This survey of existing research and statistics into “Internet Crime” has been commissioned by the National Audit Office to support its review of UK Government initiatives in reducing the impact of such crimes. The NAO’s review, by choice, excludes pure law enforcement activities but concentrates on programmes which aim at crime reduction, crime prevention and the furnishing of advice and support to potential victims.

There is no generally-agreed definition of Internet Crime as a whole, nor of the scope of many of the categories people might consider to be its constituents. The same is true its siblings, “Computer Crime”, “CyberCrime” and “E-Crime”. Indeed as we will see many of the available studies are heavily influenced by the pre-occupations of their sponsors. Thus work by children’s charities inevitably and reasonably worry about predatory sexual activity, cyber-bullying, the impact of social networking and the availability of pictures of child sexual abuse. For the banks the problems are “phishing” and various forms of credit card abuse. It is scarcely surprising that the statistics emanating from the vendors of facilities to counter computer viruses and other forms of malware concentrate on the incidence of just those forms of activity. For publishers of music, video and software the focus is on piracy. The glossily published surveys from the major management consultancies and large computer companies are designed to attract new customers and hence the enquiry base and results are mostly about hazards to larger corporations and government departments and agencies.¹

There are also situations in which “the Internet” may be blamed because it is thought to be a vector for information that may aid and incite individuals who are already vulnerable. Examples include websites and web-communities about suicide, anorexia, other forms of self-harm, and the use of weapons such as guns, knives and bombs.

¹ A similar point is made by Professor David Wall in *Cybercrime*, Polity Press, 2007, Chapter 2 *passim*

Many “internet crimes” are prosecuted as “regular” crimes and are recorded as such by the police, Home Office and Crown Prosecution Service. Often little or no distinction is made for *modus operandi*; filtering out the more traditional forms of “fraud”, child sexual abuse, etc is difficult. In so doing the opportunity to assess preventative, harm reduction, and advisory services as well as deciding on the scope of response from formal law enforcement, is lost because the data is not collected in an easily usable form.

In addition, as with many other studies of the extent of crime there are a significant number of methodological difficulties – how far does one include crimes which are suspected but never come to court – what should be the standard of proof for inclusion? Is this “proof” the act of reporting to the police or replying to a question in a survey? What fudge factors should one apply for situations where individuals *think* they have been subjected to criminal actions but have not – or where they have actually been victimised but have an inadequate realisation? What further fudge factors do you allow for unreported crimes? In relation to activities which cause distress, do you only include situations where a crime has been committed? What exactly amounts to “distress”, or to an “incident” both of which are often claimed to being measured?

There are still further problems when attempts are made to ascribe the costs of such crimes. Sums actually irretrievably lost, sums included in convictions as “taken into consideration”, sums lost but subsequently recovered, sums “at risk” (on some assessment or other) but which never left the control of the legitimate owner? Should goods be valued at their manufacturing cost, their price to wholesalers, or their retail price? How do we assess a victim’s remedial costs – say, in repairing a stolen identity, or in recovering stolen assets, or for a child that has been deeply traumatised? What allowance within remedial costs do we make for “imprudent” victims, who have not taken elementary precautions to protect themselves – or who through clumsiness actually make the situation worse? An interesting and more extensive discussion on the costs of fraud in particular appears in an ACPO publication from 2007: *The Nature, Extent and Economic Impact of Fraud in the UK*²

Finally, there are the usual problems of surveys in general: with what rigour have they been carried out? Is the methodology quantitative,

² <http://www.acpo.police.uk/asp/policies/Data/Fraud%20in%20the%20UK.pdf>, p 18 ff

qualitative, based on a literature review, or some combination? How was the sample chosen; in what sense can be said to be balanced or representative? What was the response rate? What attempts were made to test whether the respondents fully understood the questions – or used the same definitions as the survey-setters? In relation to focus groups – how were the memberships selected, and what procedures were followed to ensure that the focus group leaders/mediators did not over-influence conclusions? And where the actual results are then extrapolated to reach conclusions about wider populations, are the precise methods based on reasonable assumptions?

1.2. Scope of “Internet Crime”

One can, therefore, use definitions and the available statistics to suggest that “Internet Crime” is both insignificant and vast. In most years, convictions under the only item of legislation which is specifically targeted at “computer” crime, the Computer Misuse Act, 1990, are barely above 100.³ On the other hand, Ofcom’s 2008 *The Consumer Experience 2008 Research Report* shows that approximately 70% of the population have laptops or PCs at home and of those 93% now use Broadband. This means that 65% of adults have broadband at home.⁴ The figures from National Statistics are broadly similar.⁵ They say that in 2008, 16 million households in Great Britain (65 per cent) had Internet access. This was an increase of just over 1 million households (7 per cent) over previous last year and 5 million households (46 per cent) since 2002. Almost 16.5 million (65 per cent) UK households including Northern Ireland had access to the Internet. This was an increase of 1.2 million households (8 per cent) since 2007. Fifty-six per cent of all UK households had a broadband connection in 2008, up from 51 per cent in 2007.

Elsewhere the Ofcom Report in particular breaks these figures down by age, education and social class. (see page 35)

To an extent the raw figures disguise the impact: the growth is now taking place among the less well-educated and technologically sophisticated, those who perhaps would prefer a personal computer to be more like most other domestic appliances such as tvs, music players and radio - where the controls are minimal and easy to use and there are no security issues. Personal computers are, by their nature open programmable devices even if

³ See page 53

⁴ See page 35

⁵ See page 36

the owners don't themselves want those facilities. Openness and programmability is what gives the personal computer its incredible flexibility and adaptability. But they are also what makes it possible for many forms of computer-, cyber, and Internet-crime to succeed.

The growth of broadband provides another multiplier. When most domestic users accessed the Internet via dial-up, speeds were slower, some 10% of what is now routinely expected. This had an impact on the amount of data downloaded because customers were nearly always on a tariff where the phone calls were charged by the minute. Broadband brings much greater speeds and hence much more data per second but is also charged at a monthly flat rate. The user is now freed from the need to economise in Internet sessions. More material downloaded means more opportunity for malware to become implanted on the computers of victims. It gets worse: under dial-up the user closed down their connection to the Internet and their computer was, until the next session, isolated and therefore comparatively safe. Under broadband there is no cost to the user in keeping the connection to the Internet continuously open – and while this occurs, an unprotected computer is highly vulnerable to attack.

Not only is the personal computer an open programmable device but the Internet also derives its flexibility and ability to provide the platform for new services because it too is based on open protocols which cover both underlying technology and the means of wrapping up and transporting data.

There are yet other multipliers: more time online, more data downloaded, cheaper personal computers with cheaper data storage has enabled experimenters and entrepreneurs to launch new data-intensive services such as social networking, media downloads, more extensive e-commerce sites, more complex and sophisticated e-banking and other financial services sites. It has also prompted Government to use the Internet as a way of delivering Government services, including the collection of tax revenue and the provision of a very wide range of information services.

Many of these new services also provide a vector for criminal behaviour. Indeed although some forms of Internet crime *modus operandi* are almost invisible, others rely on masquerading as genuine Internet facilities – fake websites, misleading emails, misleading social networking connections, downloads that contain logic bombs.

Not the least of the problems is that while most people develop an instinct for personal security in terms of familiar things such as the home, walking about in the street, carrying money and high value objects, and when making purchases in shops and markets, many of the Internet environments are new. The self-protective instincts are not there, the

advice may not be there, and some of the remedies require significant technological sophistication.

It is for these reasons that “Internet Crime” is worth identifying in terms of its impact – and assessing the role of Government and Government-funded initiatives to give greater protection to the UK population.

1.3. Scope of this Study

In order for their review to have shape and produce meaningful results, the National Audit Office has decided to impose some disciplines. The scope of the study reflects NAO’s remit to assess value for money in government expenditure. Pure law enforcement activity is addressed by Her Majesty’s Inspectorate of Constabulary which covers both the police service and the Serious and Organised Crime Agency (SOCA) and is therefore omitted. A decision has also been made to exclude the problems faced by larger businesses and organisations.

The coverage therefore includes the major problems affecting lawful end-users of the Internet based in the United Kingdom. In terms of individuals who might be thought of as potential victims in need of advice and support:

- Adults, in the personal use of the Internet at home, via a work computer or while travelling, say via an Internet café or mobile-enabled computer. But excluding their pure work activities
- Children, in all their uses
- Pensioners, sometimes referred to as “silver surfers”, in all their uses
- Small Businesses (SMEs), which for this purpose are businesses with less than 50 employees

In terms of criminal activities the study includes the Internet aspects of:

- Fraud, which in turn includes such activities as “Identity Theft” and “Phishing”, E-commerce sites which do not deliver promised goods and services, the sale of misleading financial services products, fake charities seeking donations
- Malware, which is the umbrella term for viruses and Trojans, as it impacts on individuals and SMEs.

- Computer Misuse as it affects the audience indicated above; this includes unauthorised access to computers, unauthorised data modification and interference with the operation of computers
- Harassment, adult-to-adult
- “Cyber-bullying”, which is the term we will use for activities between children
- Unsolicited viewing of disturbing and illegal material, as it impacts on both adults and children
- “Grooming” of children for sexual purposes
- Exploitation of children in a retail situation
- Spam distribution
- DataTheft – the theft of proprietary and confidential information, but only as it applies to SMEs
- Denial of Service attacks, including Distributed Denial of Service attacks, but only as they apply to SMEs

The following have been excluded from this study:

- Telecommunications fraud, on the basis that the victims are more usually the telecommunications companies and that there is only a small specifically “Internet” element
- Piracy/copyright theft, on the basis that the victims are usually publishers and copyright holders of music, video and software and not the general public
- Collection and sharing of paedophile and extreme pornographic material, on the basis that although these are crimes which often have an Internet dimension this study is about victims not offenders
- Terrorism and Hactivism, on the basis that the Internet forms of these do not have much direct as opposed to indirect impact on the general public

1.4. How “Internet Crime” is dealt with in substantive laws

English statute and common law contains no direct reference to “Internet Crime” and the main category of “computer crime” is the Computer Misuse Act, 1990, as amended. But the Computer Misuse Act was designed to fill in any gaps in the existing range of offences⁶. Prosecutors have the entire range of English criminal offences from which to choose and in making their decision about precise charges they will be influenced by what they consider to be the most substantive element in the activities, the ease of obtaining reliable evidence, the impact on how a trial will be conducted, and the type of punishment available.

Many of the more reliable official statistics are based on the incidence of named offences, irrespective of *modus operandi*. As a result some understanding of the scope of the offences is essential before the limitations on the statistics can be appreciated.

1.4.1. Fraud Act 2006

Many of the offences where people lose money via Internet-related activity are caught by the Fraud Act 2006, and this covers many of its popularly-named sub-sets such as Identity Theft”, some aspects of “Phishing”, and e-commerce sites which do not deliver promised goods and services. One of the purposes of the legislation was to remove an anomaly then existing in English law that only persons and not machines (that is, computers) could be said to be “deceived”, and that had proved a limitation in terms of using the parts of the Theft Acts that referred to “deception.”⁷

The Act provides for a general offence of fraud with three ways of committing it, which are:

- by false representation,
- by failing to disclose information; and
- by abuse of position.

⁶ Law Commission Report 1989 (Law Com No 186)

⁷ :<http://www.lawcom.gov.uk/docs/cp155.pdf> paragraph 8.3

It creates new offences of obtaining services dishonestly and of possessing, making and supplying articles for use in frauds.

Formal explanatory notes to the Fraud Act can be found at:

<http://www.opsi.gov.uk/ACTS/en2006/2006en35.htm>

The Crown Prosecution Service's guidance appears at:

http://www.cps.gov.uk/legal/section8/chapter_d.html

From the perspective of computer related frauds, the most important section is section 2:

2 Fraud by false representation

- (1) A person is in breach of this section if he—
 - (a) dishonestly makes a false representation, and
 - (b) intends, by making the representation—
 - (i) to make a gain for himself or another, or
 - (ii) to cause loss to another or to expose another to a risk of loss.
- (2) A representation is false if—
 - (a) it is untrue or misleading, and
 - (b) the person making it knows that it is, or might be, untrue or misleading.
- (3) “Representation” means any representation as to fact or law, including a representation as to the state of mind of—
 - (a) the person making the representation, or
 - (b) any other person.
- (4) A representation may be express or implied.
- (5) For the purposes of this section a representation may be regarded as made if it (or anything implying it) is submitted in any form to any system or device designed to receive, convey or respond to communications (with or without human intervention).

As can be seen section 2(5) specifically addresses “systems” and “devices”. This section easily covers the operators of misleading websites and emails of almost all kinds, for example websites that purport to be banks, other financial institutions or charities, but are not. It also covers the senders of emails purporting to come from those sources. The same section will apply to offers made by websites and emails where promised goods and services are not

delivered – and also many forms of Internet auction fraud where goods are promised but there was never any intention to deliver.

Section 6 covers the use of “articles” to commit a fraud:

6 Possession etc. of articles for use in frauds

(1) A person is guilty of an offence if he has in his possession or under his control any article for use in the course of or in connection with any fraud.

Section 6 would probably apply to computer programs which enable frauds and this could refer to a website and programs to support the sending of spam and the creation and maintenance of botnets (though other laws can be used in relation to these as well). It could also apply to the equipment used to clone credit cards such as the skimmers which capture magnetic stripe data or fake fronts to ATM machines which not only capture the magnetic stripe data but may also use cameras to acquire PINs. From the perspective of the consumer, although they may know from their bank statements that their credit or debit card has been compromised, they may not know the precise means. They may also not immediately know the means by which a perpetrator sought to take advantage of the credit or debit card data. This could be by trying to make a purchase over the telephone or via a legitimate website, in which case that stage of the offence would fall within section 2 of the Fraud Act or by fabricating a fake card, which would be covered under section 6.

Section 7 makes it an offence to make, adapt, supply or offer to supply any article knowing that it is designed or adapted for use in the course of or in connection with fraud, or intending it to be used to commit or facilitate fraud. Whereas section 6 is about possessing such equipment, section 7 is about making and selling /hiring it.

Section 8 makes it entirely clear that computer programs are within the remit of the Act. Section 11 refers to “Obtaining services dishonestly”. That could include using some-one else’s genuine credit card for one’s own benefit; or by-passing encryption in order to receive a paid-for service such as satellite or cable television; or using some-one else’s genuine password in order to reach a paid-for computer service such as media downloads and online information.

Because the Fraud Act is relatively new there are few statistics so based on breach and of course no direct historic data from which to derive trends. However the best single recent attempt at looking at

the extent of fraud overall is the 2007 ACPO publication *The Nature, Extent and Economic Impact of Fraud in the UK*.⁸

There is no obligation on victims to report fraud of any kind. The City of London Police set out their criteria for case acceptance on their website⁹. Most police forces currently advise victims to report to the local police station¹⁰. Since April 2007 Online banking and card fraud should in the first instance be reported not to the police but to the relevant bank or financial institution¹¹. Since March 2009 the National Fraud Strategic Authority¹² has been in place. There is to be a National Fraud Reporting Centre. This is what the Solicitor-General said on 26 February 2009:¹³

The National Fraud Reporting Centre (NFRC) consists of an Intelligence Bureau (NFIB) and Reporting Centre.

An NFIB pilot is under way and has identified new counter-fraud intelligence, which is being investigated. Discussions are under way with potential suppliers for provision of a final solution.

The NFRC will offer the public and small businesses web and telephone-based services to report non-urgent frauds and receive fraud prevention advice. This service is planned for a national roll-out towards the end of 2009, with a regional pilot starting in summer 2009.

We can now look at some of the offences more specifically:

“Phishing”

Phishing consists of persuading some-one to give out their banking details including any passwords and then exploiting the results by raiding the bank or credit card account. The

⁸ <http://www.acpo.police.uk/asp/policies/Data/Fraud%20in%20the%20UK.pdf>

⁹ <http://www.cityoflondon.police.uk/CityPolice/ECD/Fraud/personfraud.htm>

¹⁰ <http://www.met.police.uk/fraudalert/>

¹¹ http://www.apacs.org.uk/media_centre/press/30.03.07.html

¹² http://www.attorneygeneral.gov.uk/national_fraud_strategic_authority_page.html

¹³ <http://www.publications.parliament.uk/pa/cm200809/cmhansrd/cm090226/text/90226w0016.htm>

typical method of inducing and deceiving is the alarming email purporting to come from the customer's bank (or whatever) and providing a link to a website which appears to be genuine and where the password, etc is requested. The website is fake and simply captures the information after which it can be downloaded by the phisher for later exploitation.

In practice phishing is often a crime that crosses international borders. The emails originate from overseas and the fake website is outside UK jurisdiction as well. But most domestic bank accounts, even if Internet based, will not allow payments to be made overseas – at least not without drawing attention to the fact. So, for the fraud to succeed, the final exploitation of the information requires some additional skill. The perpetrator will not want to receive funds directly into a bank account immediately traceable to him. In any event the funds will need to be moved – without leaving a trace for the authorities – to the country where the perpetrator resides.¹⁴

“Pharming” is a particular technique of phishing which involves compromising the technologies which send requests from a user to a particular website; instead of the desired website a fake fraudulent website is reached.¹⁵ From the perspective of the victim, however, the effect is the same as with the less sophisticated versions except that many conventional anti-phishing techniques fail.

What often happens is that the original phisher does not seek to remove the victims' funds himself. Using covert bulletin boards and other resources, he offers collections of valid banking information to others – at the rate of so many dollars per 100 or 1000 harvested user/password combinations. He then has his reward and moves on. The intermediary then has the problem of what is in effect a money laundering operation. He will recruit a number of “soldiers” who will set up genuine bank accounts but in

¹⁴ Herly and Florencio, *A Profitless Endeavor: Phishing as Tragedy of the Commons*, <http://research.microsoft.com/en-us/um/people/cormac/papers/phishingastragedy.pdf>; <http://www.antiphishing.org/>; http://www.cpni.gov.uk/Docs/phishing_guide.pdf;

¹⁵ http://www.cpni.gov.uk/Docs/pharming_guide.pdf

false names to receive the funds from the phished accounts. The soldiers get a percentage of the recovered funds. It is usually only the soldiers who are vulnerable to being caught because there is a trace via the banking system from the phished account to the genuine accounts but in false names that have been set up. (There are a number of variants on this scheme, mostly designed to obfuscate the transactions. Examples include fake auctions which are ended at prices no reasonable person would pay but which create an apparent reason for receiving funds. Another money laundering method involves going to a casino, purchasing chips with a credit or debit card but then cashing the chips in for cash – the “punter” never indulges in serious gambling. Both these techniques were used by a Eastern European gang based in London and operating from 2000 onwards). Many of the popular descriptions of “phishing” are misleading because they concentrate on the first stage – the design of the misleading emails and websites – and ignore the second stage – how to turn the phished details into cash.

The following offences that might have been committed along the way:

- the email which prompted the bank customers to go to the fake website would almost certainly have been sent as spam – and in order for the email to have been sent one or more computers belonging to innocent third parties would have had to be partially taken over and a rogue email program installed on them. This activity would fall within s 3 of the 1990 Computer Misuse Act – unauthorised data modification
- the fake website could fall into sections 2, 6, 7 and 8 of the Fraud Act 2006, depending on precise circumstances. There could be a further offence if the ISP providing website facilities to the phisher was deceived and/or not paid
- the person running a website, bulletin board or other facility to enable phishers to sell cards to third parties might be caught by the crime of *inciting* or

aiding and abetting offences under the Fraud Act 2006

- the “soldier” is guilty of an offence with respect to his actions in deceiving the bank under s 2 Fraud Act 2006.
- the “intermediary” would probably also be charged with conspiracy
- both the “intermediary” and the “soldiers” could also be charged with “assisting another to retain the benefit of crime”, in effect money laundering, under section 93a Criminal Justice Act 1988 (as inserted by section 29 Criminal Justice Act 1993).

But although the offences were committed, the identity of the people at the beginning of the chain will probably remain unknown. Computers used to relay spam email are usually abandoned very quickly, and all that is left are the innocent but victimised owners of those machines. Fake websites as used in phishing are likewise set up and abandoned within 24 or 48 hours. Where fake websites are operated from one country but the victims are in another the local police are not heavily motivated to respond to requests for co-operation from the law enforcement agency of another country; in event by the time the alerts arise in the form of plundered bank accounts the fake website will have disappeared days, even weeks and months before.

For all these reasons such prosecutions as exist have concentrated on the “soldiers” and occasionally their organisers. But neither of these are likely to know the identities of the original phishers.

Statistics on phishing are discussed at page 94. Counter-measures are discussed at page 97

“Identity Theft”

Although the phrase “identity theft” is widely used, in fact it encompasses a wide variety of activities, including “phishing”. It has become something of a convenient headline for a whole range of relatively conventional crimes, albeit ones carried out with greater ease because of the availability of computers and Internet-based research methods.

The European Union’s FIDIS Project has produced a series of interesting analyses:

<http://www.fidis.net/resources/deliverables/forensic-implications/#c1777>.

The perspective of the UK Home Office can be found at <http://www.identity-theft.org.uk/> . Further information can be found at

http://www.direct.gov.uk/en/RightsAndResponsibilities/DG_10031451 and this site also has links to further web-sites.

Although there is an extensive range of identity theft methodologies only some of which are Internet-based, the law is relatively simple.

In English law most forms of identity theft would now be dealt with under sections 2, 6, 7 and 11 of the Fraud Act 2006. (Fraud by Misrepresentation, Possession of Articles for Use in Frauds, Making or Adapting of Articles for Use in Frauds, Obtaining Services Dishonestly).

The Identity Cards Act, which received the Royal Assent in March 2006, creates a new criminal offence of Possession of false identity documents (s 25) . These include both the official ID card – when it has been issued – but also other existing identity documents, which could include a driving license and passport. The same Bill also creates offences of providing false information to the National Identity Register (NIR) and tampering with the NIR.

The Act’s text is at:

http://www.opsi.gov.uk/ACTS/acts2006/pdf/ukpga_20060015_en.pdf

and the explanatory notes at
<http://www.opsi.gov.uk/acts/en2006/2006en15.htm>

1.4.2. Computer Misuse, Malware, Hacking

Malware is the umbrella term for viruses and Trojans. The criminal offence is “**unauthorised data modification**” and is dealt with under section 3 Computer Misuse Act, 1990. The main practical prosecution problems are identifying the perpetrator and then making a precise link to a victim whose computer has been the subject of unauthorised data modification.

“Hacking” has no precise legal definition, but the other main element in the Computer Misuse Act is section 1, “**unauthorised access to a computer**”. The section can be used equally against the stereotypical teenage engaged in malicious recreation, staff who exceed their authority in using a company computer, and private detectives.

Most forms of computer misuse are expensive to investigate and prosecute because of the technical skills required from investigators and the frequency with which such events cross jurisdictional boundaries.

The statistics for computer misuse are discussed at page 53 and the counter-measures at page (cross-ref). Statistics for the incidence of malware comes from anti-malware vendors such as Symantec who rely on a large number of sensors to capture the incidence of each type¹⁶; however many of the viruses and Trojans identified in this way in fact cause no harm, simply because they have been detected and neutralised – see page 96.

1.4.3. Harassment, Cyber-Stalking

The Internet gives a number of opportunities to would-be cyber-stalkers, from sending large numbers of distressing emails, to putting up malicious websites, to posting information on bulletin boards, chat rooms and social networking sites, to originating misleading material which purports to come from the victim and causes them distress.

¹⁶ http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiii_04-2008.en-us.pdf

Usually these actions are offences under the Prevention from Harassment Act, 1997. The Act gives the victim the right to approach the civil courts for a restraining order but also creates a number of criminal offences. If the harassment takes place in some-one's home there is an additional offence under section 126 of Serious Organised Crime and Police Act, 2005; it is not clear whether this provision would extend to the situation where a harasser was "virtually" in some-one's home or its vicinity through the medium of a computer and telecommunications link.

More information can be found at:

<http://www.wikicrimeline.co.uk/index.php?title=Harassment>

<http://www.harassment-law.co.uk/law/act.htm>

http://www.cps.gov.uk/legal/section5/chapter_e.html

There is also a separate offence under section 43, Telecommunications Act, 1984 which covers the situation where a message is sent over a public telecommunications link that is grossly offensive or of an indecent, obscene or menacing character. But usually charges will be made on the basis of the Prevention from Harassment Act, 1997.

<http://www.statutelaw.gov.uk/content.aspx?LegType=All+Primary&PageNumber=41&NavFrom=2&parentActiveTextDocId=2232318&activetextdocid=2232391>

http://www.cps.gov.uk/legal/section12/chapter_k.html

Statistics are discussed at page 51 .

1.4.4. Disturbing and Illegal Material

The offences lie in publication, "making", "distributing" and "possessing" "obscene", "indecent" and "extreme pornographic" material. There is no offence in the publishing of material which falls short of the various statutory definitions and is merely "disturbing".

English law distinguishes between adult pornography , child pornography and extreme pornographic material. For this purpose a "child" is someone who is or appears to be under the age of 18 (s. 45 of the Sexual Offences Act 2003, until then the critical age was 16).

In terms of adult material there is no offence in simple possession – there has to be an act of publication. In the final analysis, the test of obscenity is applied by a court. Section 1(1) of the Obscene Publications Act 1959 states:

- (1) For the purposes of this Act an article shall be deemed to be obscene if its effect or (where the article comprises two or more distinct items) the effect of any one of its items is, if taken as a whole, such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it.

In practice over the years, juries have become steadily more permissive and the prosecution criteria have tended to move in step. The test for publication is:

- (3) For the purposes of this Act a person publishes an article who–
 - (a) distributes, circulates, sells, lets on hire, gives, or lends it, or who offers it for sale or for letting on hire; or
 - (b) in the case of an article containing or embodying matter to be looked at or a record, shows, plays or projects it [, or, where the matter is data stored electronically, transmits that data].

Prosecutors tend to want strong *prima facie* evidence of publication for gain, widespread offence being caused by virtue of public display, or ease of access.

Child material is dealt with under the Protection of Children Act 1978. This includes “making” (which includes downloading such material) and “distribution”. An important extension exists within s. 160 of the Criminal Justice Act 1988 – “possession”. This is a “strict liability” offence to possess “indecent” pictures (i.e. of children in a sexual situation). Strict liability means that there is enough to convict, provided that a person is found in possession of offending material and that they know that they are in possession. There are a small number of defences, which the defendant has to prove to the court on the balance of probabilities.

Since January 2009 there is a new offence of possession of “extreme pornographic images” in the Criminal Justice and Immigration Act, 2008, section 63¹⁷. Extreme pornographic images have a narrower

¹⁷ http://www.opsi.gov.uk/acts/acts2008/ukpga_20080004_en_9#pt5-pb1-11g63

definition than “obscene” for the purposes of the Obscene Publications Act. The test is:

(7) An image falls within this subsection if it portrays, in an explicit and realistic way, any of the following—

(a) an act which threatens a person’s life,

(b) an act which results, or is likely to result, in serious injury to a person’s anus, breasts or genitals,

(c) an act which involves sexual interference with a human corpse, or

(d) a person performing an act of intercourse or oral sex with an animal (whether dead or alive),

and a reasonable person looking at the image would think that any such person or animal was real.

This is too is a “strict liability” offence. Further guidance, published by the Ministry of Justice in November 2008, is available at:

<http://www.justice.gov.uk/docs/extreme-pornographic-images.pdf>

Statistics for offensive material are discussed at page 50.

1.4.5. “Grooming” of children for sexual purposes

The main offence as it applies to Internet activity is in section 15 Sexual Offences Act, 2003:

15 Meeting a child following sexual grooming etc.

(1) A person aged 18 or over (A) commits an offence if—

(a) having met or communicated with another person (B) on at least two earlier occasions, he—

(i) intentionally meets B, or

(ii) travels with the intention of meeting B in any part of the world,

(b) at the time, he intends to do anything to or in respect of B, during or after the meeting and in any part of the world, which if done will involve the commission by A of a relevant offence,

(c) B is under 16, and

(d) A does not reasonably believe that B is 16 or over.

(2) In subsection (1)—

(a) the reference to A having met or communicated with B is a reference to A having met B in any part of the world or having communicated with B by any means from, to or in any part of the world;

(b) “relevant offence” means—

(i) an offence under this Part,

(ii) an offence within any of paragraphs 61 to 92 of Schedule 3...

The “relevant offences” include sexual activity with a child (section 9), “causing or inciting a child to engage in sexual activity” (section 10), “engaging in sexual activity in the presence of a child” (section 11), “causing a child to watch a sexual act” (section 12), and “arranging or facilitating commission of a child sexual offence” (section 14).

As can be seen these sections can also be used where, for an example, an adult is conversing with a child via a social networking site, or using Instant Messaging; such activities include of course, the use of still and moving photographic material for example via web-cams.

Statistics on sex offenders in general are discussed at page 65.

1.4.6. Exploitation of Children in a retail Internet situation

There is no specific UK legislation to meet this threat. The US has the Children’s Online Privacy Protection Act, 1998 (“COPPA”). It applies to the online collection of personal information by persons or entities within U.S. jurisdiction from children under 13 years of age. It details what a website operator must include in a privacy policy, when and how to seek verifiable consent from a parent or guardian, and what responsibilities an operator has to protect children's privacy and safety online including restrictions on the marketing to those under 13. Details can be found at:

<http://www.ftc.gov/os/1999/10/64fr59888.pdf>.

The Office of Fair Trading, OFT, has powers to investigate (http://www.oft.gov.uk/advice_and_resources/resource_base/legal/) under, among other things, Consumer Credit Act, 2006, Enterprise Act, 2002 (which includes provisions for consumers codes of practice) and Unfair Terms in Consumer Contracts under a SI from 1999 (<http://www.opsi.gov.uk/si/si1999/19992083.htm>).

I have not been able to find any reliable statistics to cover this situation.

1.4.7. Spam Distribution

Spam is unsolicited bulk e-mail. It is often claimed that over 90 per cent of all email traffic consists of spam. A more detailed explanation can be found at the Spamhaus website¹⁸. There has been an English criminal offence of sending spam since December 2003. It appears in The Privacy and Electronic Communications (EC Directive) Regulations 2003, sections 22 and 23.

<http://www.opsi.gov.uk/si/si2003/20032426.htm>. Section 22 requires that electronic mail for marketing purposes can only be sent if the recipient's consent has been obtained. That consent can be obtained when some-one purchases goods and either ticks (or fails to untick) a box indicating consent. Section 23 forbids the sending of direct marketing emails where the sender's identity is disguised or concealed.

The Regulations also cover unsolicited phone calls and fax messages. Enforcement lies not with the police but the Information Commissioner.

http://www.ico.gov.uk/what_we_cover/privacy_and_electronic_communications/enforcement.aspx and http://www.ico.gov.uk/for_the_public/topic_specific_guides/spam_emails.aspx

However much spam originates outside the UK and indeed outside the European Union; moreover, the Information Commissioner does not really have adequate resources.

Spam is often sent via a computer not belonging to the originator but which has been hi-jacked for the purpose and a rogue email program installed. From the perspective of the spammer this has the advantage of low cost and increased difficulty in being traced. An offence under s 3 Computer Misuse Act takes place in these circumstances, but the absence of evidence and the difficulties of identifying perpetrators means that law enforcement agencies seldom take investigations very far.

Statistics are discussed at pages 66 and 70.

¹⁸ <http://www.spamhaus.org/definition.html>

1.4.8. DataTheft

Datatheft is the theft of proprietary and confidential information. In the SME situation, the most typical modus operandi does not involve the Internet – data in the form of documents, databases, designs, pictures, etc is copied to a USB stick, external disk drive or burnt to CD or DVD. In a variant the stolen data can be emailed to outside the organisation and in those circumstances can be thought to have an Internet dimension.

More sophisticated technical means include “hacking” a website which has been poorly secured, either to see information which is supposed to be protected by password access or where commands are used which enable an entire “back-end” database to be retrieved (this technique has been used by fraudsters seeking customer credit card data). A trojan or “back-door” program can be covertly installed on a target computer to give a user access via the Internet. Alternatively, a key-logging device or program can be installed on a target computer, either to capture a username/password combination for later use or for immediate acquisition of confidential information that was being typed into the computer. A further technique involves the exploitation of poorly secured wireless networks and then hoping that computers on the network are themselves poorly secured.

English law does not have a specific criminal offence relating to industrial espionage or theft of trade secrets but does provide criminal sanctions via common modus operandi. There are also routes via the civil courts and these include the ability of a claimant to ask for a Civil Search Order.

The legal “problem” is that data is not “property” or “tangible” in English law, which means it cannot be stolen for the purposes of the Theft Acts. The classic case of *Oxford v Moss* [1979] 68 Cr.App.R. 183 concluded that although the medium upon which data is held - paper, a disk – can be stolen – the data itself cannot.

There are recommendations dating from 1997 by the Law Commission, the body that exists to suggest changes to the law, for an English law of trade secrets - http://www.lawcom.gov.uk/misuse_trade.htm but these have never been followed up by legislation.

The indirect routes to criminal prosecution include:

- unauthorised access to a computer (s 1 CMA, 1990) where, for example, a computer is accessed locally without authorisation and data removed
- unauthorised access to a computer (s 1 CMA, 1990) where some-one takes advantage across the Internet of a poorly secured web-site
- unauthorised data modification (s 3 CMA, 1990) where back-door or remote control program is installed without authorisation and used to siphon off information
- data interception (s 1 RIPA, 2000) where data traffic is subjected to interception on a network
- fraud by false representation (s 2 Fraud Act 2006) where some-one rings up and asks for information while purporting to be some-one who would entitled to such information
- the use of audio probes – “bugs” – would be an offence under the Wireless Telegraphy Act, 1949, if the bug used a radio transmitter

If the information stolen is “personal data”, then there can be protection under the Data Protection Act, 1998, section 55:

Unlawful obtaining etc. of personal data

- (1) A person must not knowingly or recklessly, without the consent of the data controller—
- (a) obtain or disclose personal data or the information contained in personal data, or
 - (b) procure the disclosure to another person of the information contained in personal data.
- (2) Subsection (1) does not apply to a person who shows—
- (a) that the obtaining, disclosing or procuring—
 - (i) was necessary for the purpose of preventing or detecting crime, or
 - (ii) was required or authorised by or under any enactment, by any rule of law or by the order of a court,
 - (b) that he acted in the reasonable belief that he had in law the right to obtain or disclose the data or information or, as the case may be, to procure the disclosure of the information to the other person,
 - (c) that he acted in the reasonable belief that he would have had the consent of the data controller if the data controller had known of the obtaining, disclosing or procuring and the circumstances of it, or
 - (d) that in the particular circumstances the obtaining, disclosing or procuring was justified as being in the public interest.
- (3) A person who contravenes subsection (1) is guilty of an offence.

- (4) A person who sells personal data is guilty of an offence if he has obtained the data in contravention of subsection (1).
- (5) A person who offers to sell personal data is guilty of an offence if—
 - (a) he has obtained the data in contravention of subsection (1), or
 - (b) he subsequently obtains the data in contravention of that subsection.
- (6) For the purposes of subsection (5), an advertisement indicating that personal data are or may be for sale is an offer to sell the data.
- (7) Section 1(2) does not apply for the purposes of this section; and for the purposes of subsections (4) to (6), “personal data” includes information extracted from personal data.

Protective measures are discussed at page 96.

1.4.9. DoS, DDoS, Botnets, Extortion

Extortion is usually addressed via the offence of blackmail

Computer-related extortion is technically relatively easy to execute. The problem facing all blackmailers is how to collect the “reward” without identifying yourself so that you are caught.

A Denial of Service (DoS) attack consists of one computer sending another a rapid series of requests which the second “target” computer cannot process properly and as a result ceases to work. In a Distributed Denial of Service (DDoS) attack several computers working together send the commands to the “target” computer. From the perpetrator’s perspective DDoS had advantages over simple DoS in that the chances of overwhelming the target are much greater and much more difficult to stop. If the attack comes from just one computer, then traffic from it can be filtered by reference to its IP address. If multiple computers are involved blocking by IP address is much more difficult.

In a Botnet, large collections of computers are used to mount the attack. The setting up of a botnet typically requires the would-be owner – “bot-herder” in the jargon - to send out large numbers of emails which contain back-door programs through which each computer can be controlled. Alternatively the back-door may be picked up from a malicious website. Many of these attempts at installing covert back-doors will fail because they are identified by anti-virus programs and/or the owner is suspicious of the email or website by which they arrive. Each of these taken-over computers is sometimes referred to as a “zombie” Once a large number of computers have been compromised by the success of the back-door program, the botnet owner then runs a “herding”

program which issues simultaneous commands to all compromised computers.¹⁹

The following laws are involved:

- for a simple DoS attack. For a while there was doubt whether this was an offence, as the target computer was not obviously “accessed” (the test in section 1 Computer Misuse Act 1990) nor subject to “authorised data modification” (the section 3 test). However in its revised form, section 3 should get a prosecutor a conviction – section 36 Police and Justice Act 2006.
- in a DDoS attack and to create a Botnet the perpetrator has to arrange to set up a rogue program on third party computers – a clear instance of an offence under s 3 CMA 1990.
- but the perpetrators of most blackmail and extortion attempts are at their most vulnerable when they try to collect the money they seek. The normal criminal offence is under s 21 of the Theft Act 1968:

The Theft Act, 1968 says

s 21. Blackmail

(1) A person is guilty of blackmail if, with a view to gain for himself or another or with intent to cause loss to another, he makes any unwarranted demand with menaces; and for this purpose a demand with menaces is unwarranted unless the person making it does so in the belief-

(a) that he has reasonable grounds for making the demand; and

(b) that the use of the menaces is a proper means of reinforcing the demand.

(2) The nature of the act or omission demanded is immaterial, and it is also immaterial whether the menaces relate to action to be taken by the person making the demand.

(3) A person guilty of blackmail shall on conviction on indictment be liable to imprisonment for a term not exceeding fourteen years.

¹⁹ More information on botnets can be found at: <http://www.honeynet.org/papers/bots/>; http://www.sans.org/reading_room/whitepapers/malicious/1299.php; <http://www.shadowserver.org/wiki/pmwiki.php?n=Information.Botnets> and, with the usual cautions about Wikipedia, at: <http://en.wikipedia.org/wiki/Botnet> which contains a number of useful onward references.

<http://www.statutelaw.gov.uk/content.aspx?LegType=All+Legislation&title=Theft&searchEnacted=0&extentMatchOnly=0&confersPower=0&blanketAmendment=0&sortAlpha=0&TYPE=QS&PageNumber=1&NavFrom=0&parentActiveTextDocId=1204238&ActiveTextDocId=1204267&filesize=2351>

Statistics on the extent of botnets can be seen, among others, at the ShadowServer website.²⁰

²⁰ <http://www.shadowserver.org/wiki/pmwiki.php?n=Stats.Statistics>

2 Research Sources

2.1. Statistics: Quantitative Research

For the reasons rehearsed in the Introduction, there are few reliable statistics sets which refer directly to “Internet Crime”. There is no single clear unchallenged definition of “Internet Crime” and indeed the same is true of most of the activities that might be considered its constituents. Crimes are most readily defined by the precise laws under which they can be prosecuted but often the authorities concentrate on breach by legal offence rather than *modus operandi*. The problems become more acute once one moves from “offences notified” or “offences prosecuted” or “convictions” to the world of suspicion but not proof that an offence has occurred, or calculations about what might be going on but is not reported.

In their *Personal Internet Security Report*,²¹ the House of Lords Science and Technology Select Committee said: “(para 2.28) Still less clear is the scale of online fraud and theft. The problem here is compounded by the lack of clear definitions that might help to differentiate online fraud from “traditional” fraud. For example, Tim Wright, of the Home Office, asked how many prosecutions there had been for “e-crimes”, responded, “Not only do the police databases not distinguish between whether crimes are committed electronically or not, but nor do the Prosecution or the Home Office figures distinguish between the two. So we do not know how many people have been prosecuted for e-crimes as distinct from offline crimes”

This means that any picture of “Internet Crime” has to be built up indirectly from statistics collected for related purposes. Here there are further traps unless the limits of the methodologies used in each study are carefully understood. It is all too easy to take figures from one survey (with a sample drawn from a non-representative sub-group and where the sample cannot be said to be in any way balanced) and multiply the result with other figures purportedly showing the total population at risk and then producing results which please lazy journalists but no one else.

²¹ <http://www.publications.parliament.uk/pa/ld200607/ldselect/ldsctech/165/165i.pdf>

2.1.1. Statistics on General Internet Usage and Growth

There are two reliable statistical sources and two that are useful for further background.

Ofcom’s The Consumer Experience 2008 Research Report

The Report²² covers the delivery of the various forms of tv service and mobile telecommunications as well as pc/internet. The research methodologies are explained at p 133ff and are based on a continuous quarterly face-to-face survey with a balanced sample of just over 2000.

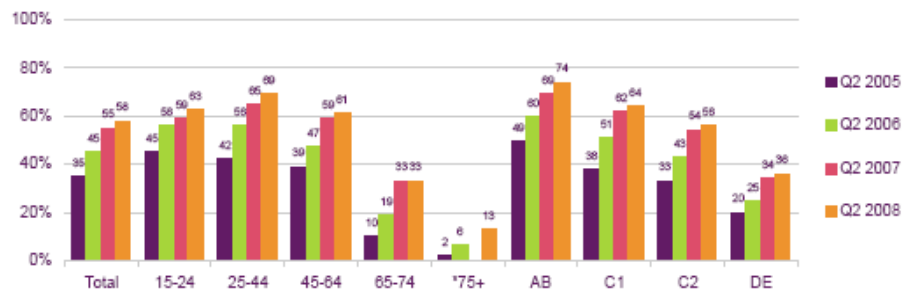
Approximately 70% of the population have laptops or PCs at home and of those 93% now use Broadband. This means that 65% of adults have broadband at home . Ofcom also has socio-economic, income and educational and regional profiles and also international comparisons). Here are two sample charts:

Figure 32: Ownership of PCs or laptops in the home



* Data for 2006-2008 based on Q2, all other data based on Q4
 Base: All adults 15+
 Source: Ofcom communications tracking survey

Figure 43: Age and socio-economic profile of those who have broadband access at home



* Small base size treat as indicative only
 Base: All adults (Q2 2005, 2206) (Q2 2006, 2439) (Q2 2007, 2265) (Q2 2008, 2109)
 Source: Ofcom communications tracking survey

²² <http://www.ofcom.org.uk/research/tce/ce08/research.pdf>; Section starts at 4.2.13;

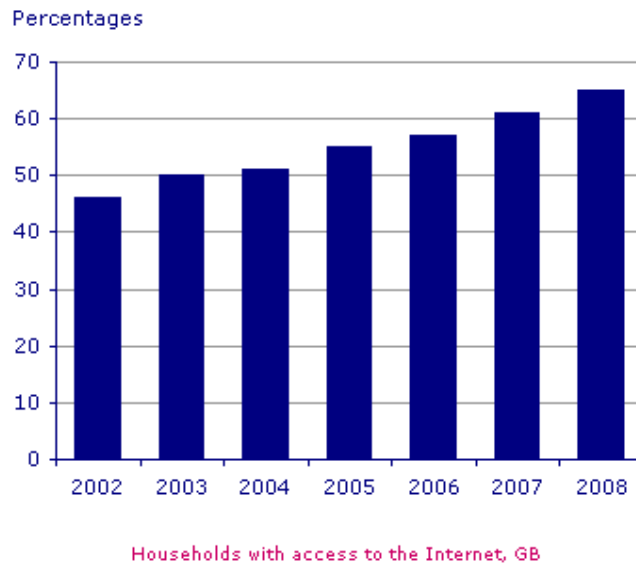
Use of the Internet from any location as opposed to just in the home is at 71%. The other locations include work, libraries, internet cafes and at the houses of friends. Over-75s remain the least likely group to have internet at home, and also the least likely to own a PC – just under a fifth of this age group have access to a home PC. Broadband ownership among over-75s stands at 13%, just over twice the level reported in 2006.

The Ofcom statistics enable us to see the sorts of people who might be at risk from various Internet-related crimes in terms of wealth, age and education

National Statistics

Their figures align reasonably closely with those from Ofcom²³:

Internet Access 65% of households had access in 2008



In 2008, 16 million households in Great Britain (65 per cent) had Internet access. This is an increase of just over 1 million households (7 per cent) over the last year and 5 million households (46 per cent) since 2002. Estimates for

²³ <http://www.statistics.gov.uk/CCI/nugget.asp?ID=8>

Great Britain are provided to give a time series, as UK estimates are not available prior to 2006.

Almost 16.5 million (65 per cent) UK households including Northern Ireland had access to the Internet. This was an increase of 1.2 million households (8 per cent) since 2007. The region with the highest level of access was the South East with 74 per cent. The region with the lowest access level was the North East with 54 per cent.

Fifty-six per cent of all UK households had a broadband connection in 2008, up from 51 per cent in 2007.

Adults under 70 years of age who had a degree or equivalent qualification were most likely to have access to the Internet in their home, at 93 per cent. Those individuals who had no formal qualifications, were least likely to have an Internet connection in their home at 56 per cent.

ONS has also produced a *Survey of E-Commerce 2007* – Internet sales rose by 30% in 2007 compared to 2006 (£163 bn compared with £125.2 bn) ²⁴

Key findings of the survey include:

- Internet sales represented 7.7 per cent of the total value of all sales by non-financial sector businesses in 2007.
- Internet sales accounted for 39.3 per cent of the value of sales over all ICTs in 2007, up from 35.7 per cent in 2006.
- 30.4 per cent of the value of all purchases made by non-financial sector businesses were made over the Internet or other ICTs in 2007.
- 60.8 per cent of businesses used the Internet to interact with public authorities, such as government departments and local and regional authorities in 2007, an increase of nearly 18 per cent since 2006.
- 70.3 per cent of businesses had a website

²⁴ <http://www.statistics.gov.uk/pdffdir/ecomnr1108.pdf>

There are significant differences in the rate of adoption of newer ICTs between the largest and smallest businesses. Supply chain management systems were used by 33.4 per cent of businesses with 1000 or more employees in 2007, compared with only 4.2 per cent of businesses with 10 to 49 employees

Symantec Online Living Report

This 2009 report²⁵ from a malware vendor is designed to “monitor and provide insight into rapidly changing technology, Internet usage and the social impact on individuals and families”. It is based on 9000 interviews in 12 countries, and covers the extent of email usage, social networking, webcams, photo-sharing and twitter-like services. The survey was carried out by a company called Harris Interactive and is honest about the extent of possible error. (see p 8)

- Email is the baseline with 92% using it to communicate with friends and family
- 42% use webcams, with very high usage in China (74%), India (68%), Brazil (66%) and France (53%)
- Half of adults use social networking
- 7 in 10 access photos online and use IM
- 24% use a Twitter-like service
- 86% of kids send text messages
- 73% of kids email from their phones
- 23% are using a Twitter-like service
- Kids on average are spending 3 hours/week texting: kids in the U.S. text the most at 10 hours/week, while kids in Japan and Germany text the least at 1 hour/week vs. adults who spend 2 hours/week texting
- 92% of kids socialize with family and friends online, approximately 5 hours a week

²⁵ http://www.nortononlineliving.com/documents/NOLR_Report_09.pdf;
http://www.nortononlineliving.com/documents/NOLR_studyreport031609.pdf/

- 55% of kids have made friends online, up from 45% of kids in countries surveyed last year and have an average of 37 online friends. U.S. kids have the most friends at 82, and kids in Japan have the fewest at 13

APACS

APACS, the trade association for bank payment services, and whose fraud figures are considered elsewhere at page 55 produce one further interesting “trends” statistic: “From 2001 to 2008... the total value of online shopping transactions alone increased by 524 per cent (up from £6.6 billion in 2001 to £41.2 billion in 2008).²⁶

2.1.2. Statistics on the use of the Internet by Children

UK Children Go Online

Sonia Livingstone in her *UK Children Go Online Report*²⁷ of 2005 bases her figures based on 14 focus groups, a national in-home 40-minute face-to-face survey of 1511 9-19 year olds and 906 parents of the 9-19 year olds and 13 further focus groups. She says:

“Nearly all children and young people (98%) have used the internet: 75% of 9-19 year olds have accessed the internet from a computer at home, and school access is near universal (92%); 36% have more than one computer at home, 24% live in a household with broadband access; and 19% have internet access in their bedroom. Access platforms are diversifying, with children’ having computers (71%), mobile phones (38%), digital television (17%) and games consoles (8%) with internet access. Socioeconomic

²⁶ http://www.apacs.org.uk/media_centre/press/06_07_11.html

²⁷ <http://www.lse.ac.uk/collections/children-go-online/End%20of%20Award%20Report,%20UK%20Children%20Go%20Online,%20Sonia%20Livingston.pdf>

differences are sizeable: 88% of middle class though only 61% of working class children have accessed the internet at home. Use is fairly frequent: 9-19 year olds are divided between daily users (41%) and weekly users (43%); however, some make low (13%) or no (3%) use of the internet. Of these, 47% of low/non-users say that they lack access, 25% are not interested, 15% don't know how to use it, and 14% lack the time. Most 9-19 year olds are online for less than an hour – still less than they watch television or listen to music: 19% spend about ten minutes per day online and 48% between half an hour and one hour. Of 9-19 year olds who go online daily or weekly, 90% use it for school/college work, 94% for information, 72% to send emails, 70% to play games, 55% to send instant messages and 45% to download music. Further, 44% look for information on careers/education, 40% look for products/shop online, 26% read the news and 21% use chat rooms. Some use it for less-approved activities: among 12-19 year olds who go online daily or weekly, 21% admit to copying schoolwork, 8% claim to have hacked, 5% visited a dating site, 4% have sent a hostile/bullying message and 2% visited a gambling site”

She also reports:

The risks of undesirable content

More than half have seen pornography online (57% of 9-19 year old daily and weekly users), mostly unintentionally: 38% of 9-19 year old regular users have seen a pornographic pop-up advert while doing something else, 36% have accidentally found themselves on a porn site when looking for something else, and 25% have received pornographic junk mail. Parents and children agree that the internet is more likely to expose children to pornography than are television, video or magazines. Further, 22% of 9-19 year old daily and weekly users who have accidentally ended up on a site with violent or gruesome pictures, while 9% have found a site hostile or hateful to a group of people.

However, the survey and, especially, the focus group findings reveal mixed responses to online porn: more than half claim not to be bothered by it, but a sizeable minority are upset or disgusted. Interestingly, 45% of 18-19 year old internet users who have seen any pornography (on/offline) think they were too young to have seen it when they first did.

The risks of online communication

One third of 9-19 year old daily and weekly users have received unwanted sexual (31%) or nasty comments (33%) online or by text message, though only 7% of parents are aware that their child has received sexual comments and only 4% that their child has been bullied online. Also important is the frequency with which children divulge personal information online: 46% say that they have given out personal information to someone that they met online; further, 40% say that they have pretended about themselves online.

Although most children are aware, from media coverage, of the risks of meeting people they don't know, 30% have made an online acquaintance, and 8% say they have met face to face with someone whom they first met online. Nonetheless, follow up questions reveal that the vast majority told a friend or parent and, generally, went with a friend to the meeting, resulting in few less than positive meetings.

Multivariate analyses show that social-psychological factors, family communication

patterns and gender all play a role in the interaction risks that are taken by teens online. While line psychological characteristics of the teens affect the frequency of online communication and of having online friends, offline confidence influences whether they look for personal advice or meet people offline. Offline family communication patterns and parental attitudes towards the internet and other media also had an impact on communication online by young people.

NSPCC

Overall key child protection statistics have been compiled from a variety of sources by the NSPCC and can be found at: http://www.nspcc.org.uk/Inform/resourcesforprofessionals/Statistics/KeyCPStats/keycpstats_wda48731.html and http://www.nspcc.org.uk/Inform/resourcesforprofessionals/Statistics/KeyCPStats/6_wda48742.html

However it will be seen that many of these figures are not especially up-to-date and other than references to the availability of abusive images. There are a number of attitudinal analyses, which are discussed separately.

Eurobarometer: Towards a safer use of the Internet in the EU - a parent's perspective

This parent-orientated study²⁸ was pan-European and is considered in more detail later for its qualitative content. Its main quantitative findings are:

The number of children using the Internet varied considerably across Europe. The proportion of parents who thought that their child used the Internet was the lowest in Italy (45%), Greece and Cyprus (both 50%). In all other Member States, at least two-thirds of the parents answered that, as far as they knew, their child used the Internet: from 68% in Portugal to 94% in Finland.

Looking at both children's and parents' Internet usage, similarities existed in the country breakdown: for both, the same countries appeared at the higher and lower ends of the distribution. The correlation coefficient for the relationship between the proportion of online parents and children was .64 – a moderately-strong correlation between the two variables at the country level.

Half of the parents who did not use the Internet themselves said that their child had online access. Nine out of 10 children – who were Internet users – accessed it from home.

Older children were more likely to use the Internet on their own computer at home (47% of 15-17 year-olds vs. 22% of

²⁸ http://ec.europa.eu/information_society/activities/sip/eurobarometer/index_en.htm

6-10 year-olds), at school (57% vs. 49%), at a friend's place (32% vs. 16%) or in an Internet café (6% vs. 1%).

CEOP

CEOP seem only publish data about their own activities (<http://www.ceop.gov.uk/mediacentre/statistics.asp>), eg 131 children have been safeguarded from sexual abuse either directly or indirectly as the result of CEOP activity – of which 18 have been identified through the examination of child abuse images; 297 arrests have been made as a result of CEOP activity. 6 organised paedophile rings have been dismantled or disrupted as a result of CEOP activity. Since its launch, the **Thinkuknow** education programme has reached 1.7 million children and young people between the ages of 8 and 16 years across all parts of the UK.

Internet Watch Foundation

The Internet Watch Foundation (IWF) publishes²⁹ statistics about the number of reports received and the number of offending sites: “ During 2007, the IWF processed 34,871 reports which resulted in 2755 top level domains with child sexual abuse content being assessed, confirmed as potentially illegal, traced, and the appropriate intelligence being disseminated accordingly. There has been a 10% rise in the number of reports processed compared to 2006 figures which we believe is due to increased awareness of our ‘Hotline’ and conscientious action by the public. However, there has been a 15% decrease in the number of individual web pages and a 10% decrease in the number of domains depicting child sexual abuse. We hope this shows that fewer internet users are actually being inadvertently exposed to confirmed child sexual abuse images. Indeed, if

29

[http://www.iwf.org.uk/documents/20080417_iwf_annual_report_2007\(web\).pdf](http://www.iwf.org.uk/documents/20080417_iwf_annual_report_2007(web).pdf)

this is the case, the UK can be proud of efforts by many of the IWF's funding members in trying to protect their customers from such exposure by voluntarily committing to blocking access to child sexual abuse URLs on the IWF list. It is also a testament to the online sector's continuing support of IWF activities that UK hosted child sexual abuse content remains negligible and on the rare occasion it is traced to networks in the UK, is removed within hours.

IWF is a hotline service – see page 100.

2.1.3. Statistics about use of Internet by older-consumers

Use of Internet by Older Consumers (Ofcom: The Communications Market 2008):³⁰

Function	All adults who use the internet	Adults aged 65+ who use the internet
Use email to contact friends and relatives	91%	90%
Transfer photos from a digital camera or mobile phone to a computer	83%	72%
Buy things over the internet	81%	68%
Install security features like a firewall, anti-spy or antivirus software	79%	58%
Find out about local services including the council, hospital, leisure facilities and so on	76%	67%
Install software on a computer which can control or block access to certain websites	74%	53%
Do my banking over the internet	58%	41%
Listen to radio over a computer	43%	15%
Join in debates about subjects that interest me through posting comments on websites	33%	11%
Any of these	97%	93%
Mean number of functions of interest	6.2 (out of 9)	4.8 (out of 9)

Source: Ofcom research

In terms of how the over-65's actually use the internet (rather than what interests them) there are marked differences from the UK average. For almost all activities, use by older consumers was lower than average, the exceptions being for online transactions and accessing the news, where usage levels were similar. In line with the average for all internet users, the most popular use of the internet was for communication purposes, with 63% of older internet users using it to keep in touch. The largest disparities between usage levels were for finding

³⁰ <http://www.ofcom.org.uk/research/tce/ce08/research.pdf> see para 1.4.8 ff

work/studies information, where only 18% of internet users aged 65+ had used the web compared to almost half (48%) of all internet users and for creativity (4% of users aged 65+ compared to 22% of all internet users).

2.1.4. Statistics on Social Networking

Neither Ofcom nor National Statistics cover the relatively new phenomenon of social networking. International data is available from Nielsen: its 2009 Report *Global Faces and Networked Places* says³¹ : “While two-thirds of the global online population already accesses member community sites, their vigorous adoption and the migration of time show no signs of slowing. Social networking will continue to alter not just the global online landscape, but the consumer experience at large... Facebook - the world’s most popular social network - is visited monthly by three in every 10 people online... One in every 11 minutes online globally is accounted for by social network and blogging sites....The social network and blogging audience is becoming more diverse in terms of age: the biggest increase in visitors during 2008 to “Member Community” Web sites globally came from the 35-49 year old age group³²

Social Networking is significant in the “Internet Crime” domain because people often provide a great deal of information about themselves to the public-at-large – and this provides fraudsters with the raw material with which to carry out various forms of identity theft. It can also provide a vector for harassment (cross-ref) and grooming (cross-ref). GetSafeOnline’s 1997 ICM survey covers some aspects of this.

Some commentary on social networks is provided by CEOP³³, considered later in this Review.

³¹ http://blog.nielsen.com/nielsenwire/wp-content/uploads/2009/03/nielsen_globalfaces_mar09.pdf

³² http://en-us.nielsen.com/etc/content/nielsen_dotcom/en_us/home/news/news_releases/2009/march/social_networks_mbc.92241.RelatedLinks.86876.MediaPath.pdf;

³³ http://www.ceop.gov.uk/downloads/documents/socialnetwork_serv_report_221206.pdf

2.1.5. Crime Statistics

British Crime Survey

The BCS seeks to measure the amount of crime in England and Wales periodically by asking around 50,000 people aged 16 and over, living in private households, about the crimes they have experienced in the last year. Since 2001 it is now carried out on a continuous basis. In 2006 the Home Office published *Fraud and Technology Crimes as Online Report 09/06*.³⁴ This was a “thematic” report rather than a regular one, with no immediate plans to repeat it, though it is likely that something similar will come in the future. In turn it relies on the BCS 2003/4 and 2004 Offending, Crime and Justice Survey 2004. BCS asks a “few” Internet-related questions in its regular surveys, but is constrained by a belief that BCS interviews should not last beyond 45 minutes and there are always many other items on the agenda fighting for space.

Looking first at fraud in all its forms, in 2004/05, 278,902 fraud and forgery offences were recorded by the police, a decrease of 12 per cent from the previous year when 317,947 fraud and forgery offences recorded (Nicholas *et al.*, 2005). However, many crimes of this kind are not reported to the police because either victims are not aware of the incident, or if they are aware, they are more likely to report it to their bank or card-holder company. The Home Office Report goes on to cite figures from the Association of Payment Clearing Services (APACS) : “recent figures have shown that total card fraud was £219.4million for the period January to June 2005, significantly (13%) lower than in the same time period in 2004. The main reason for this is due to the introduction of chip and pin technology where cardholders have to use their pin number instead of their signature. However, Internet, phone and mail-order fraud was the only type of fraud to have increased in the same time period (APACS, 2005).”³⁵

³⁴ <http://www.homeoffice.gov.uk/rds/pdfs06/rdsolr0906.pdf>

³⁵ See page 55 for more up-to-date APACS figures.

Turning now to the Internet dimension, *Fraud and Technology Crimes* says: “The 2003/04 BCS found that 51 per cent of adults aged 16 years or above had personally used the Internet to either send emails or access Internet websites (either at home or outside the home, including at work). Levels of personal Internet access in the 2003/04 BCS have risen slightly since the 2002/03 BCS (from 46% to 51%). However, the OCJS figures were stable between the 2003 and 2004 surveys for those aged 10 to 25, at around 91 per cent. The 2003/04 Omnibus Survey found that 58 per cent of people living in England and Wales had used the Internet in the 12 months prior to interview; this is in line with the findings from the 2003/04 BCS.” The more up-to-date figures from Ofcom appear at page 50).

Over half (54%) of adults in the 2003/04 BCS who had used the Internet, said they had used a payment card in order to buy goods or services over the Internet. This is a significant increase from 49 per cent in the 2002/03. Among Internet users who had not bought goods or services over the Internet the most common reason given for not doing so was concern about security (72%); or worry about entering personal details online (37%). Preferring to see the actual product before purchasing (22%) was another common concern. Those who did shop online were asked what precautions they took to secure their details on the Internet. The vast majority in the 2003/04 BCS (97%) said they took some measures; this was the same as in the 2002/03 BCS. The most popular precaution was to look for a secure site to buy from (73% mentioned this). Over a half said they only used well-known sites or companies (53% and 56% respectively).

The BCS did not provide information on experience of Internet fraud. However, figures from the OCJS found that among 12- to 25-year-olds, of the one per cent who reported using someone else’s card details, only a small minority had obtained the details over the Internet (0.1% of all those aged 12 to 25 years old) and similarly a small minority reported buying goods/services over the Internet using someone else’s card details without the card owner’s permission (0.1% of 12- to 25-year-olds). Both these figures are

probably too small to be useful. At a BCS sample size of 50,000, 0.1% means 50 people.

Computer Viruses

Based on BCS 2003/04, just over a quarter (27%) of individuals who used the Internet at home reported that their home computer had been affected by a computer viruses in the last 12 months, significantly higher than for 2002/03 BCS (18%). Nine per cent of those who used the Internet reported that a computer virus had damaged the computer and 18 per cent reported the computer had been infected with a computer virus but had not actually been damaged. Of those individuals who had experienced a computer virus, whether it damaged the computer or not, nearly four in ten (37%) said they had reported this to someone. Of those who had reported the virus to somebody, nine per cent said they had reported it to an Internet service provider, six per cent to either a website administrator or a systems administrator and only one per cent to the police. According to the 2004 OCJS, one per cent of those aged 10 to 25 years who had used the Internet reported having sent a computer virus in the last 12 months. Males were more likely than females to report this activity (2% versus 1%) and 10- to 17-year-olds were more likely than 18- to 25-year-olds (2% and 1% respectively). The percentage of young people reporting sending a virus was stable between the 2003 and 2004 OCJS. It should be noted that due to the nature of these offences one offender can impact on multiple victims.

The **BERR/PWC 2008 Report** considered in more detail at page 58 and which is focused on “incidents” in larger organizations said³⁶: “ Only 14% of UK companies had a malware infection last year, down from 35% two years ago. Even among very large businesses, less than half had an infection

³⁶ [http://www.pwc.co.uk/pdf/BERR_ISBS_2008\(sml\).pdf](http://www.pwc.co.uk/pdf/BERR_ISBS_2008(sml).pdf)

last year. It appears that there are three main reasons why fewer malware infections are being reported:

- Corporate anti-virus defences have significantly improved;
- Most minor virus infections no longer register in the same way as they did. They are no longer considered security breaches but as events dealt with by routine controls; and
- Malware itself and the motivation of its writers have changed.

“Law enforcement in this area has improved around the world. As a result, the kudos derived from writing a disruptive worm is outweighed by the personal consequences. Instead, virus writers are increasingly employed by organised crime to write stealthy code that seeks to obtain confidential data or open holes in security for hackers to exploit. Spyware now accounts for one in six of the worst infections. Malware infection used to be the end goal; now, it is merely the first step, enabling other more lucrative attacks.”

Computer Hacking

In two per cent of the 2003/04 BCS households which had used the Internet at home, someone had accessed or hacked into files on their home computer in the last 12 months. Victims were less likely to report these incidents than computer virus incidents, with 13 per cent reporting the incident to someone. Of those who reported being a victim of hacking, 33 per cent reported this to a website administrator and 27 per cent to an Internet service provider. From the 2004 OCJS, one per cent of those aged 10 to 25 years who had used the internet in the last 12 months reported using a computer to access another's computer's files without permission. Males (2%) were significantly more likely to report this than females (1%) and 10-to 17-year-olds were

more likely than those aged 18 to 25 to report this offence. Between 2003 and 2004 these levels of computer hacking remained the same.

Figures for the numbers of prosecutions under the Computer Misuse Act are given at page 53

Offensive Material

The 2003/04 BCS asked adults who had used the Internet at home whether they were worried about their household unwittingly accessing or receiving offensive, pornographic or threatening material over the Internet and whether or not they had actually done so.

One-third (34%) of home Internet users said they were worried about their household accessing or receiving offensive, pornographic or threatening material over the Internet on their home computer (11% very worried and 23% fairly worried). Women were slightly more likely to be worried than men (36% versus 33%). People in households with children were particularly likely to be worried (45% those in households with children; 27% those in other households). Worry was also higher amongst Asian groups (46%) and those between 25 and 65 years of age (38%). Based on BCS 2003/04, one quarter (25%) of people who used the Internet at home had unwittingly accessed or received offensive or upsetting unsolicited material via the Internet in the 12 months prior to interview, significantly higher than in 2002/03 BCS (21%). The percentage of males and females who reported receiving offensive material was the same at 25 per cent. Those aged 25 to 44 years using the Internet at home were significantly more likely to report receiving this type of material than those aged 16 to 24 years, as were Whites (compared with BMEs) and individuals with qualifications (compared with those without).

Just under a fifth (18%) of Internet users who had reported receiving offensive or upsetting unsolicited

material via the Internet reported it to someone, the most common being an Internet service provider (8%) followed by a website administrator (7%). Only two per cent reported receiving offensive messages to the police. Based on the 2004 OCJS three per cent of 10- to 25-year-olds reported that they had visited a website on how to commit crime; one per cent of 18- to 25-year-olds said they had visited a racist website (this question not asked to those aged under 18). Similar to other technology activities, males were more likely than females to report to having visited these websites and the levels were stable between 2003 and 2004.

These figures are worth comparing with statistics from the **Internet Watch Foundation**.³⁷ See page 43.

Harassment

Fraud and Technology Crimes says that from the BCS, 12 per cent of individuals who used the Internet said they had personally received a message by email that they considered offensive or constituted harassment. Of those who had received an offensive email, nearly a third (31%) reported the incident to someone. Of those who reported the incident, one in seven (15%) reported it to a systems administrator (15%) and a further 13 per cent reported it to a website administrator. Older individuals (40- to 65-year-olds) were more likely to be victims of email harassment than any other age group (13% compared to 10% for 16- to 39-year-olds). However, among mobile phone users, younger people (16- to 25-year-olds) were more likely (10%) than older people (aged 26 and above 8%) to be victims of mobile phone harassment.

Based on 2003/04 BCS, nine per cent of individuals who had used a mobile phone reported having

³⁷ [http://www.iwf.org.uk/documents/20080417_iwf_annual_report_2007_\(web\).pdf](http://www.iwf.org.uk/documents/20080417_iwf_annual_report_2007_(web).pdf)

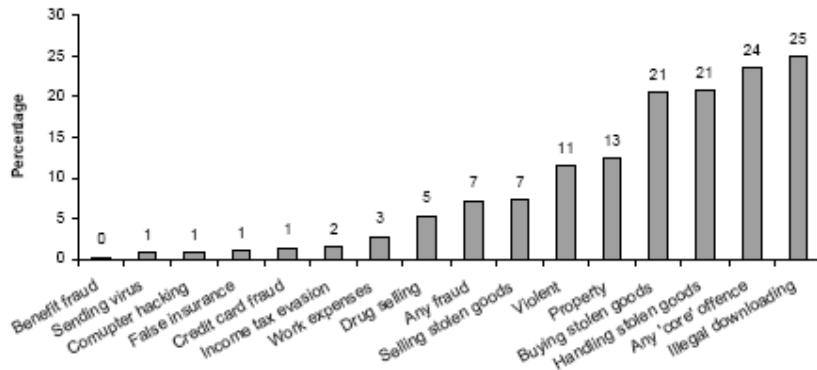
received a voice or text message that they considered to be offensive or a form of harassment in the last 12 months (5% text only, 4% voice only and 1% both). Men and women were equally likely to report being victims of these types of harassment. According to the 2004 OCJS, only one per cent of 10- to 25-year-olds who used the Internet said that they had sent an email message in order to harass, scare or threaten. This compares with five per cent of mobile phone users in the same age group who said they had sent a voice or text message to someone in order to harass, scare or threaten them in some way. Younger people (aged 10 to 15) were more likely than young adults (aged 16 to 25) to report that they had sent harassing emails. The opposite was found for mobile phone harassment where young adults were more likely than children to report to this. Levels of reporting of both email and mobile phone harassment were broadly stable between the 2003 and 2004 survey.

Not all the activities respondents were asked about are illegal – see page 23.

Technology Offences seen in relation to other forms of Youth Offending

Fraud and Technology Crimes also provides a useful chart showing the role of “technology offences seen in relation to other forms of youth offending:

Figure 2.2: Prevalence of offences in the last 12 months among all 18- to 25-year-olds (2004 OCJS)



Notes:

1. Violent includes: robbery, assault with and without injury.
2. Property includes: burglary, vehicle-related theft, criminal damage and other thefts.
3. Any 'core' offences include: violent offences, property offences and drug selling.

Computer Misuse Act statistics

The figures below are for *convictions* under the 1990 Computer Misuse Act. Please see page 23 for how the Act works; essentially it was designed to criminalise situations not already covered by existing law such as that for theft, fraud and criminal damage. The figures do not differentiate by type of perpetrator so that, for example, the employee who exceeds his authority to use a corporate computer is not distinguished from a teenage recreational hacker.

Volume of offences under the Computer Misuse Act 1990				
Magistrates' Court (MC)				
Act and Section	Nov 2004-Oct 2005	Nov 2005-Oct 2006	Nov 2006-Oct 2007	Nov 2007-Oct 2008*
Computer Misuse Act 1990 { 1(1) }	7	10	16	46
Computer Misuse Act 1990 { 2(1)(a) }	10	14	10	7
Computer Misuse Act 1990 { 2(1)(b) }	21	7	7	26
Computer Misuse Act 1990 { 3(1) }	43	18	26	30

* (data may be subject to amendment)

GetSafeOnline

Identity Theft Statistics

A **Home Office** study (Statistical Bulletin 10/07) dealt with Mobile phone theft, plastic card and identity fraud, and is based on the 2005/06 BCS: *Mobile phone theft, plastic card and identity fraud: Findings from the 2005/06 British Crime Survey*³⁸

It found: “Overall 94 per cent of adults had never had their personal details used without permission in any of the ways listed. For those adults who were victims of ID fraud, the most common experience was the use of credit or debit cards to make a purchase without the person’s knowledge (4%). One per cent of adults had *ever* experienced criminals applying for and obtaining a credit card and one per cent had experience of others obtaining a loan, mortgage or credit agreement using their personal details without their permission. With respect to all adults, the proportion who had their personal details used *in the last year* was two per cent, with just one per cent of adults having experienced criminals using a plastic card to make a purchase without their permission in the same time period. Less than half of one per cent said that their ID was used without their permission in other ways, for example, to apply for a credit card, mobile phone contract, state benefits, or to open a bank or building society account. None had experienced having their personal details used *in the last year* to apply for a driving licence or passport, to their knowledge (Table 3.5). Of those who had *ever* experienced having their ID used without their permission, the majority (68%) reported that this had happened on only one occasion; one in five (19%) reported that this had happened on three or more occasions.

In their *Personal Internet Security Report*, the **House of Lords Science and Technology Select Committee** said: “Figures on the scale of the problem are hard to come by. Indeed, the lack of data on identity theft is symptomatic of a

³⁸ <http://www.homeoffice.gov.uk/rds/pdfs07/hosb1007.pdf>

lack of agreed definitions or detailed statistics on almost all aspects of Internet security. In February 2006 the Financial Services Authority estimated the cost of identity fraud to the United Kingdom economy at £1.7 billion per annum. But this included over £500 million losses reported by APACS, the United Kingdom payments association, covering counterfeit cards, lost or stolen cards, card not present fraud, through to full account takeover (the latter put at just £23.8 million). It also included £215 million for missing trader VAT fraud, £395 million for money-laundering and even £63 million for the anti-fraud procedures in the UK passport office. It is impossible to deduce from these figures how much online identity theft costs the United Kingdom economy. (House of Lords Science and Technology Committee 5th Report of Session 2206-7, Personal Internet Security Vol 1 , para 2.27)³⁹

This is what **APACS** said for 2007: ⁴⁰

- In 2007, total card fraud losses increased by 25% to £535 million.
- The success of chip & PIN has meant that over the past three years losses on transactions on the UK high street have reduced by 67% from £218.8m in 2004 to £73.0m last year.
- Mail-non-receipt fraud also fell, dropping 34%, and lost and stolen card fraud showed an overall decrease on 2006 of 18%.
- In 2007, counterfeit card fraud increased by 46% to £144.3 million. However, despite this fraud decreasing domestically by 32%, the overall figure increased due to fraudsters copying UK cards and using these stolen cards in countries which do not yet have chip and PIN.
- The main area of card fraud to rise in 2007 was card-not-present (CNP) fraud. This increased by 37% compared with 2006. However, these losses need to be considered in the context of huge increases in both the number of people shopping online and over the phone, and the number of retailers offering telephone or online

³⁹ <http://www.publications.parliament.uk/pa/ld200607/ldselect/ldscitech/165/165i.pdf>;

http://www.apacs.org.uk/resources_publications/documents/FraudtheFacts2007.pdf

⁴⁰ (http://www.apacs.org.uk/resources_publications/card_fraud_facts_and_figures.html):

shopping. Since 2000, CNP losses have risen by 298%, but over the same time period the total value of online shopping transactions increased by 87%.

Here are the **APACS** 2008 statistics⁴¹:

Card Fraud Type – on UK issued credit and debit cards	2004	2005	2006	2007	2008	+/- (07/08)
Phone, internet and mail order fraud (Card-not-present fraud)	£150.8m	£183.2m	£212.7m	£290.5m	£328.4m	+13%
Counterfeit (skimmed/cloned)fraud	£129.7m	£96.8m	£98.6m	£144.3m	£169.8m	+18%
Fraud on lost or stolen cards	£114.4m	£89.0m	£68.5m	£56.2m	£54.1m	-4%
Card ID theft	£36.9m	£30.5m	£31.9m	£34.1m	£47.4m	+39%
Mail non-receipt	£72.9m	£40.0m	£15.4 m	£10.2m	£10.2m	0%
TOTAL	£504.0m	£439.4m	£427.0m	£535.2m	£609.9m	+14%
Contained within this total:						
UK retail face-to-face transactions	£218.8m	£135.9m	£72.1m	£73.0m	£98.5m	+35%
UK cash machine fraud	£74.6m	£65.8m	£62.0m	£35.0m	£45.7m	+31%
Domestic/International split of total figure:						
UK fraud	£412.3m	£356.6m	£309.9m	£327.6m	£379.7m	+16%
Fraud abroad	£92.5m	£82.8m	£117.1m	£207.6m	£230.1m	+11%
Online banking fraud losses	£12.2m	£23.2m	£33.5m	£22.6m	£52.5m	+132%
Cheque fraud losses	£46.2m	£40.3m	£30.6m	£33.5m	£41.9m	+25%

⁴¹ http://www.apacs.org.uk/09_03_19.htm

As can be seen, phone, internet and mail order fraud are all dealt with as a single phenomenon. However in the Report for the previous year, 2007, APACS suggests that the Internet element of card-not-present fraud was 73% of the total. They go on to say: “The vast majority of this type of fraud involves the use of card details that have been fraudulently obtained through methods such as skimming, bin-raiding, data hacking or through unsolicited e-mails or telephone calls. The card details are then used to make fraudulent card-not-present transactions, most commonly via the internet.”

References by APACS to the Internet tend to be about advice for merchants using credit card facilities over the Internet as opposed to advice for consumers.

US statistics on “Identity Theft” are published by the **Federal Trade Commission**: <http://www.ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2008.pdf>. FTC has set up a “Consumer Sentinel Network” which is an online database of consumer complaints. During 2008 they received some 1.2 million such complaints. In relation to “Identity Theft”, the Report says:

Credit card fraud (20%) was the most common form of reported identity theft followed by government documents/benefits fraud (15%), employment fraud (15%), and phone or utilities fraud (13%). Other significant categories of identity theft reported by victims were bank fraud (11%) and loan fraud (4%). Government documents/benefits fraud is now the second most common reported type of identity theft after credit card fraud. Fraudulent tax return-related identity theft, a subtype of government documents/benefits fraud, has increased nearly six percentage points since calendar year 2006. Electronic fund transfer-related identity theft continues to be the most frequently reported type of identity theft bank fraud during calendar year 2008, despite declining since calendar year 2006.

Symantec, in its *Global Internet Security Threat Report*, also attempts to deal with Identity Theft, but says that the biggest threat is via the transporting away of data stored on disk and USB stick media. The *Report* is considered in more detail at page 67.

2.1.6. Business Orientated Statistics

By and large business-orientated statistics are concerned more with identifying security threats (as they affect business) and with the deployment of remedies. Only one of the sets identified is specific to smaller businesses and that is defective in that it was based on voluntary responses to an online questionnaire

BERR information security breaches survey 2008 ⁴²

This is the most recent in a survey series which started in 1991 when it was sponsored by the old DTI (BERR's predecessor) and carried out by the National Computing Centre (NCC). The survey is focussed on "security incidents" occurring in UK businesses of all sizes. There were 1007 telephone-based interviews each lasting 20 minutes. Respondents were asked about "attitudes" towards information security, "security awareness" the existence of policies and particular facilities, etc. The notion of what constitutes an "incident" remains opaque. The statistics on security breaches appear at page 22 of the survey report. One interesting observation is that: "There is some evidence that management is becoming desensitized to minor incidents in well-understood areas, such as systems failure and virus infection. Companies no longer regard these as security breaches, but as routine events swept up by business-as-usual controls without needing to be logged. It will also be seen that the survey covers "systems failure or data corruption" which is of course is non-criminal. There are undoubtedly insights in the report that are extremely useful to medium and large companies. However there is relatively little of direct value to the current NAO review.

⁴² [http://www.pwc.co.uk/pdf/BERR_ISBS_2008\(sml\).pdf](http://www.pwc.co.uk/pdf/BERR_ISBS_2008(sml).pdf)

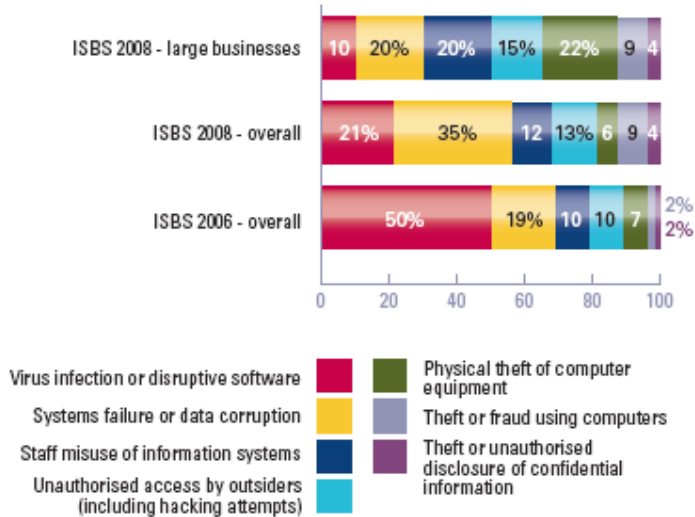
	Small (<50 staff)	Large (>250 staff)	Very Large (>500 staff)
Companies that had a security incident in the last year	45%	72%	96%
Average number of incidents, median (mean)	6 (100)	15 (200)	>400 (>1,300)
Average cost of worst incident in year	£10k to £20k	£90k to £170k	£1m to £2m

Confidential information is increasingly at risk, especially in large businesses, where:

13%	have detected unauthorised outsiders within their network.
9%	had fake (phishing) emails sent asking their customers for data.
9%	had customers impersonated (e.g. after identity theft).
6%	have suffered a confidentiality breach.

What was the worst security incident faced by UK businesses?

Figure 57



CSI Survey 2008 ⁴³

CSI – Computer Security Institute - is a US membership group for computer security professionals. Its statistics are very widely quoted, partly because its earlier work was co-sponsored by the FBI. The survey population is from US corporations, government agencies, financial institutions, medical institutions, and universities. In 2008, the 13th year of the survey series, some 522 “security practitioners” were consulted. This was a 10% response rate as 5000 questionnaires were sent out. The survey admits that it is informal and skewed because the correspondents are actively interested in security issues. The pre-occupations are fairly close to that of the BERR/PWC survey in the UK and similarly only indirectly relevant to the current work of NAO. The table below is useful to the extent of indicating the range of threats as seen by this particular community:

⁴³ <http://www.gocsi.com/>

Figure 13: Percentages of Key Types of Incident

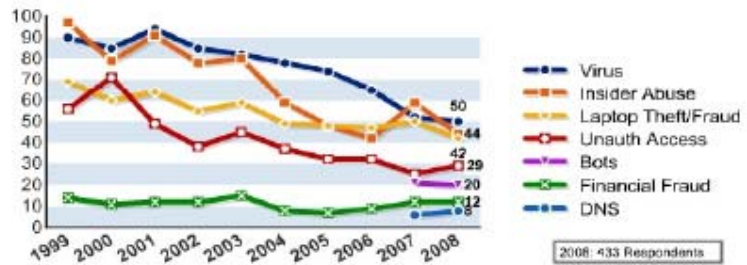


Table 1	2004	2005	2006	2007	2008
Denial of service	39%	32%	25%	25%	21%
Laptop theft	49%	48%	47%	50%	42%
Telecom fraud	10%	10%	8%	5%	5%
Unauthorized access	37%	32%	32%	25%	29%
Virus	78%	74%	65%	52%	50%
Financial fraud	8%	7%	9%	12%	12%
Insider abuse	59%	48%	42%	59%	44%
System penetration	17%	14%	15%	13%	13%
Sabotage	5%	2%	3%	4%	2%
Theft/loss of proprietary info	10%	9%	9%	8%	9%
from mobile devices					4%
from all other sources					5%
Abuse of wireless network	15%	16%	14%	17%	14%
Web site defacement	7%	5%	6%	10%	6%
Misuse of Web application	10%	5%	6%	9%	11%
Bots				21%	20%
DNS attacks				6%	8%
Instant messaging abuse				25%	21%
Password sniffing				10%	9%
Theft/loss of customer data				17%	17%
from mobile devices					8%
from all other sources					8%

CIFAS 2008 Fraud Report⁴⁴

CIFAS is a not-for-profit membership association dedicated to the prevention of financial crime and staff fraud. CIFAS provides a range of fraud prevention services to its

⁴⁴ http://www.cifas.org.uk/default.asp?edit_id=896-57

Members, including a fraud avoidance system used by the UK's financial services companies and public authorities. It currently has 270 members. Its website says: "Members of CIFAS are required to operate effective in-house procedures to enable fraud or attempted fraud to be identified and classified. Basic information on each case is filed on the CIFAS database. The information is then transferred electronically to a number of Participating Agencies (Callcredit, Equifax, Experian, Experian Decision Analytics and Synectics Solutions Ltd).

"When a Member searches the CIFAS database through one of the Agencies, the Member is made aware of the need to investigate by means of a flagged warning. The Member is then required to conduct an investigation into the case and not just reject the application or account/product/facility/insurance policy/employment, as it may be a genuine application rather than one submitted by a fraudster. This warning does not mean that the individual has been blacklisted. It means that extra precautions should be taken to ensure that the application or facility that has prompted the check is genuine and this protects the individual from further fraud."

The methodology does not appear to be able to pick up frauds by individuals against individuals or situations where the victims are small business and who are unable to recover their losses from the sort of entities that are members of CIFAS.

CIFAS's statistics do not separately identify computers or the Internet as a *modus operandi*:

2. The following tables show a summary of the statistics and the number of fraud cases recorded by CIFAS Members during 2008, broken down by the type of fraud identified. Definitions are given below the table.

	Jan to Dec 2007	Jan to Dec 2008	% Change
Fraud cases identified	185,003	214,342	15.86%
Financial Benefit/Losses avoided	£987,829,077	£848,304,084	-14.12%

Fraud Cases Identified refers to each proven instance of fraud identified by CIFAS Members and filed to the CIFAS database. Members must have sufficient evidence to take the case to the police although it is not mandatory that they do so. A fraud case can involve multiple subjects and multiple addresses.

Financial Benefits. This is the amount of money that Members of CIFAS reported that they have saved through being alerted to previous frauds by CIFAS warnings.

	Jan to Dec 2007	Jan to Dec 2008	% Change
Identity Fraud - Granted	32,175	34,011	5.71%
Identity Fraud - Not Granted	45,418	43,631	-3.93%
Identity Fraud - Total	77,593	77,642	0.06%
Application Fraud - Granted	14,515	15,055	3.72%
Application Fraud - Not Granted	62,355	61,968	-0.62%
Application Fraud - Total	76,870	77,023	0.02%
False Insurance Claim	390	433	11.03%
Facility Takeover Fraud	6,272	19,275	207.32%
Asset Conversion	478	522	9.21%
Misuse of Facility	23,400	39,447	68.58%
Victims of Impersonation	65,066	62,658	-3.70%
Victims of takeover	6,106	19,290	215.92%
Protective Registrations	32,982	49,061	48.75%

Identity Fraud cases include cases of false identity and identity theft.

Application Fraud/False Insurance Claim relates to applications or claims with material falsehood (lies) or false supporting documentation where the name has not been identified as false.

Facility Takeover Fraud occurs where a person (the 'facility hijacker') unlawfully obtains access to details of the 'victim of takeover', namely an existing account holder or policy holder (or of an account or policy of a genuine customer or policy holder) and fraudulently operates the account or policy for his own (or someone else's) benefit.

Asset Conversion relates to the sale of assets subject to a credit agreement where the lender retained ownership of the asset (for example a car or a lorry).

Misuse of Facility is where an account, policy or other facility is used fraudulently.

Garlik in their 2008 report⁴⁵ (cross-ref) rely quite heavily on CIFAS figures but claim to be able to extract the "cybercrime" element. See page 71.

Ernst & Young: 2008 Global Information Security Survey

46

This survey was conducted by "Ernst & Young professionals" in over 50 countries to 1400 organisations. Respondents were typically Chief Information Officers or staff concerned with information system security. The pre-occupations are those of very large companies.

⁴⁵ http://www.garlik.com/static_pdfs/cybercrime_report_2008.pdf

46

[http://www.ey.com/Global/assets.nsf/International/TSRS_Global_Information_Security_Survey_2008/\\$file/TSRS_Global_Information_Security_Survey_2008.pdf](http://www.ey.com/Global/assets.nsf/International/TSRS_Global_Information_Security_Survey_2008/$file/TSRS_Global_Information_Security_Survey_2008.pdf)

FSA Financial Risk Outlook 2009

This survey does not address Internet as a delivery mechanism other than in relation to Iceland (at p 19)

http://www.fsa.gov.uk/pubs/plan/financial_risk_outlook_2009.pdf

Federation of Small Businesses: Inhibiting Enterprise 2008⁴⁷

The Federation of Small Businesses - FSB - carried out an online survey over 2 weeks with 1823 responses. The respondents to the survey were, in the main, self employed (32%) or micro businesses with 1-4 employees (42%) or those with 5-9 employees (15%) and 10-25 employees (8%). In terms of their location, survey respondents were spread across England, Scotland and Wales but with strong representation from the South East (22%) and South West (18%). Responses spanned a whole range of industry sectors but the largest response was from the retail sector in particular at 17%. The main claim is that 54% of businesses have been a victim of fraud or online crime in the last twelve months: 37% had an issue with phishing emails, 15% were victim to card not present fraud and 15% experienced IT system issues (such as viruses, hacking etc).

The survey methodology is undoubtedly disappointing but there are some useful insights, for example on reporting:

“Of those businesses that had experienced fraud or online crime: 50% said that they had reported it to their bank or relevant financial institution, 20% said they had reported it to the police or Crimestoppers and 33% said that they did not report it. Businesses said that the main reasons for not reporting fraud or online crime were that it ‘would not achieve anything’ (23%), that the ‘police would not be interested’ (14%) and that they would ‘not be able to find the fraudsters’ (8%) Businesses also did not report because they thought the crime was not serious enough (10%) and that they were not sure who to contact (7%) and were

⁴⁷ <http://www.fsb.org.uk/policy/assets/inhibitingenterprise.pdf>

concerned that the police would not even want to accept the report.”



2.1.7. Statistics about Cyber-Stalking

There appear to be no reliable UK-based statistics on cyber-stalking and most of the UK NGOs which specialise in this subject point to a US-based NGO called WHO@ - Working to Halt Online Abuse: <http://www.haltabuse.org/>⁴⁸ However their figures are based on those who agreed to complete an online questionnaire on their website. WHO@ admit that while they receive 50-75 cases a week of online harassment, in each recent year the number of filled-in questionnaires has varied from 200 to 450.

2.1.8. Statistics about Sex Offenders

In 2001, the Multi-Agency Public Protection Arrangements – MAPPA – was set up under the Criminal Justice and Courts’ Services Act 2000. In 2006 it reported on its first 5 years of activity: <http://www.probation.justice.gov.uk/files/pdf/MAPPA%20-%20The%20First%20Five%20Years.pdf>. The report contains statistics about total numbers of Registered Sex Offenders and, separately, “Violent Offenders”. For example in 2005/6 there were

⁴⁸ <http://www.haltabuse.org/resources/stats/index.shtml>

29973 Category 1 Registered Sex Offenders. All those convicted of “possessing” or “making” indecent photographs of children are required to be registered for a minimum of 5 years. But the Report contains no reference to the incidence of Internet or online activity.

2.1.9. Statistics about Obscene Publications

The following is from Hansard 20 Feb 2008 column WA73:

The Attorney-General (Baroness Scotland of Asthal): The Crown Prosecution Service (CPS) captures some information on the volume of prosecution of specific offences in its Offence Based Universe of the Compass Management Information System. These records have existed only since April 2004, following the full implementation of the Compass system.

The records show that there have been no offences contrary to the Children and Young Persons (Harmful Publications) Act 1955 recorded since April 2004. The number of offences contrary to the Obscene Publications Acts 1959 and 1964 recorded between 1 April 2004 and 1 February 2008 are as follows:

Obscene Publications Act 1959 {2(1)}	441
Obscene Publications Act 1964 {2}	3

This will of course cover adult material; no breakdown is available to show how much of this was the result of online activity; presumably the other offences include printed and video material.

2.1.10. Statistics about the incidence of malware and spam

As well as statistics from victims, some of the major vendors of protective services are able to collect data from their own “alarm” computers. In addition some vendors offer “out-sourced” malware and spam prevention so that all relevant traffic aimed at a client first goes through facilities owned by the vendor so that the traffic can be

“cleaned.” Symantec, for example, produces a “*Global Internet Security Threat Report*”⁴⁹ It is based on 40,000 sensors in over 180 countries. As will be seen, some of the threats discussed in the report are not about malware but such things as loss of data through the theft of data-carrying media

These are the highlights:

Attack Trends Highlights

- During this reporting period, the United States accounted for 31 percent of all malicious activity, an increase from 30 percent in the first half of 2007.
- The United States was the top country of attack origin in the second half of 2007, accounting for 24 percent of worldwide activity, a decrease from 25 percent in the first half of 2007.
- The education sector accounted for 24 percent of data breaches that could lead to identity theft during this period, more than any other sector. This was a decrease from the previous reporting period, when it accounted for 30 percent of the total.
- Government was the top sector for identities exposed, accounting for 60 percent of the total, a significant increase from 12 percent in the first half of 2007.
- Theft or loss of computer or other data-storage medium was the cause of the most data breaches that could lead to identity theft during this reporting period, accounting for 57 percent of the total. It accounted for 61 percent of the identities exposed in the second half of 2007, more than any other sector.
- The United States was the top country for hosting underground economy servers, accounting for 58 percent of the total identified by Symantec, a decrease from the first half of 2007, when it accounted for 64 percent of the total.
- Bank accounts were the most commonly advertised item for sale on underground economy servers known to Symantec, accounting for 22 percent of all items, an increase from the first half of 2007, when they made up 21 percent.

⁴⁹ http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiii_04-2008.en-us.pdf.

- Symantec observed an average of 61,940 active bot-infected computers per day in the second half of 2007, an increase of 17 percent from the previous period.
- The average lifespan of a bot-infected computer during the last six months of 2007 was four days, unchanged from the first half of 2007.
- The United States had the most bot-infected computers, accounting for 14 percent of the worldwide total, a slight increase from 13 percent in first half of 2007.
- Madrid was the city with the most bot-infected computers, accounting for three percent of the worldwide total.
- In the last six months of 2007, Symantec identified 4,091 bot command-and-control servers. This is an 11 percent decrease from the previous reporting period, when 4,622 bot command-and-control servers were identified. Of these, 45 percent were located in the United States, more than any other country.
- The United States was the country most frequently targeted by denial-of-service attacks, accounting for 56 percent of the worldwide total. This is a decrease from 61 percent reported in the first half of 2007.

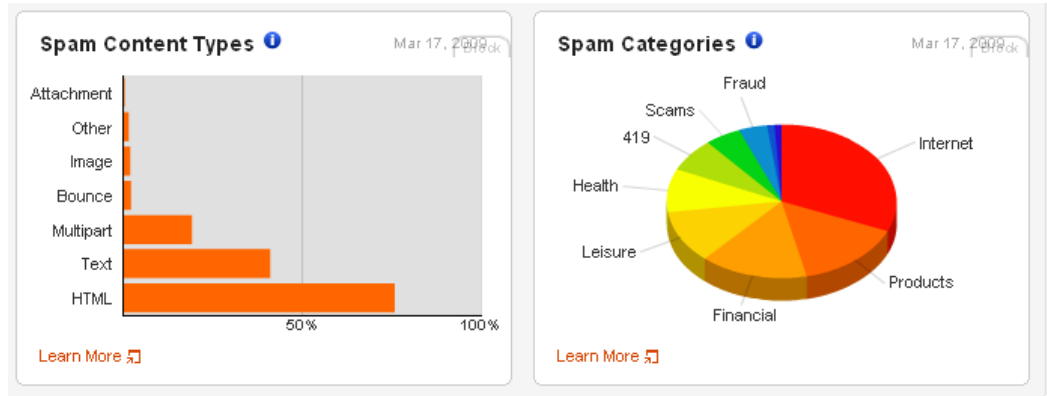
Malicious Code Trends Highlights

- In the second half of 2007, 499,811 new malicious code threats were reported to Symantec, a 136 percent increase over the first half of 2007.
- Of the top 10 new malicious code families detected in the last six months of 2007, five were Trojans, two were worms, two were worms with a back door component, and one was a worm with a virus component.
- During the second half of 2007, Trojans made up 71 percent of the volume of the top 50 malicious code samples, a decrease from 73 percent in the first six months of 2007.
- Forty-three percent of worms originated in the Europe, Middle East, and Africa (EMEA) region.
- North America accounted for 46 percent of Trojans for this period.

- Threats to confidential information made up 68 percent of the volume of the top 50 potential malicious code infections reported to Symantec.
- Of all confidential information threats detected this period, 76 percent had a keystroke logging component and 86 percent had remote access capabilities, a decrease for each from 88 percent in the previous period.
- Forty percent of malicious code that propagated did so through executable file sharing, a significant increase from 14 percent in the first half of 2007, making this the most commonly used propagation mechanism during this period.
- Seven percent of the volume of the top 50 malicious code samples modified Web pages this period, up from three percent in the previous period.
- During the second half of 2007, 10 percent of the 1,032 documented malicious code samples exploited vulnerabilities. This is lower than the 18 percent proportion of the 1,509 malicious code instances documented in the first half of 2007.
- Seven of the top 10 staged downloaders this period were Trojans, two were worms, and one was a worm with a viral infection component.
- Of the top 10 downloaded components for this period, eight were Trojans and two were back doors.
- Malicious code that targets online games made up eight percent of the volume of the top 50 potential malicious code infections, up from five percent in the previous period.

Symantec also provide details about spam:

http://www.symantec.com/business/security_response/landing/spam/index.jsp?inid=us_ghp_staticpromo_spam_trends



Spamhaus hosts the ROSKO list (Register of Known Spam Operations)⁵⁰ and says that 80% of known spam operations come from just 100 sources:

80% of spam received by Internet users in North America and Europe can be traced via aliases, addresses, redirects, locations of servers, domains and DNS setups, to a hard-core group of around 100 known spam operations, almost all of whom are listed in the ROKSO database.

Each spam operation, or "spam gang", consists on average of between 1 to 5 spammers (giving an estimated total of 300-400 spammers).

The majority of the spammers on the ROKSO List operate illegally and move from network to network and country to country seeking out Internet Service Providers with poor security or known for not enforcing of anti-spam policies.

Many of these spam operations pretend to operate 'offshore'. Those who don't hide behind anonymity pretend to be small 'ISPs' themselves, claiming to their providers that the spam is being sent not by them but by non-existent 'customers'. When caught, almost all use the age old tactic of lying to each ISP long enough to buy a few days or weeks more of spamming and when terminated simply move on to the next ISP already set up and waiting.

ROKSO is a "3 Strikes" register. To be placed on the ROKSO list a spammer must first be terminated by a minimum of 3 ISPs for AUP⁵¹ violations. Once listed in ROKSO, IP addresses under the

⁵⁰ <http://www.spamhaus.org/roko/index.lasso>

⁵¹ Acceptable Use Policy

control of ROKSO-listed spammers are automatically and preemptively listed in the Spamhaus Block List

2.1.11. Other Reports

MacAfee 2009 Predictions

http://www.mcafee.com/us/local_content/reports/2009_threat_predictions_report.pdf

McAfee is another anti-malware company that is in a position to collect data, from its own Avert Labs. However the name of the report is “Threat Predictions 2009” and its main purpose is to warn rather than provide solid statistics

Garlik UK Cybercrime Report 2008

This is a report from a computer security vendor and where the actual work was carried out by a company called 1871 Ltd.⁵² It covers “cybercrime” rather than “Internet Crime” and seeks to aggregate existing statistics to reach rather startling conclusions:

	2007	2006	Change
Identity theft and identity fraud	84,700	92,000	-8%
Financial fraud	255,800	207,000	+24%
Offences against the person	2,240,000	1,944,000	+15%
Computer misuse (excluding viruses)	132,800	144,500	-8%
Sexual offences	830,000	850,000	-2%
Total	3,543,300	3,237,500	+9%

⁵² http://www.garlik.com/static_pdfs/cybercrime_report_2008.pdf

One has to turn to the appendices to see how Garlik and 1871 Ltd have managed to take statistic sets which were collected on a basis which did not distinguish between online and conventional *modus operandi* so that the “cyber” or “Internet” aspect could be isolated. In relation to “Identity theft and identity fraud”, for example, we are told that “40% are facilitated online”. But the source for this is 117 interviews with “convicted and unconvicted fraudsters” over a 3-year period between 2003 and 2006. There is no indication of how this sample was chosen.

Again figures for “computer misuse” seem to have been derived by looking at the number of VAT-based enterprises in the UK and then taking the figure of “just under 50% of UK industries experienced a security incident” from the BERR/PWC Study – see page 58 - to achieve a multiplier. The result is the claim that 830,000 UK businesses experienced a security incident of which 417,000 were serious. But as we have seen, the BERR/PWC study contains no clear definition of “security incident” but which must include rather more than “computer misuse” and the Garlik calculations take no account of the variations in size of a business in the way in the BERR/PWC study does.

And again looking at sexual offences, a rough figure from the Internet Crime Forum that 1 in 5 children using chatrooms have been approached by paedophiles and other undesirables while online is used as the basis for another calculation. Garlik assume that 60% of children between 5 and 15 access the Internet, say that there are 6,922,300 children aged between 5 and 15 creating a total of 4,153,000 who access the Internet. The 1 in 5 figure gives 830,000 cases of “unwanted sexual approaches in 2007”.

The **Internet Crime Forum** paper is presumably *ChatWise, StreetWise* from March 2001⁵³. This paper is much more cautious. It says: “It is extremely difficult to make any accurate assessment of the level of sexual approaches to children in chat rooms in the UK, since uniform crime

⁵³ http://www.internetcrimeforum.org.uk/chatwise_streetwise.pdf

figures do not record any distinction between online and offline cases. In order to make an accurate estimate of the extent of the problem of children being the target of sexually inappropriate approaches on the Internet, it would be helpful to categorise crime reporting figures in this way. In addition, reports of incidents which do not lead to criminal charges are not recorded, whether they take place in a children's playground or on the Internet." It goes on to cite some individual examples and then quote from a number of attitudinal surveys such as one by Readers' Digest/Mori in 2000, NOP/kids.net and a telephone-based survey from the Crimes Against Children Center at the University of New Hampshire. The *Internet Safety Technical Task Force* Report from Berkman (considered later, see page 91) criticizes a number of these "attitudinal" surveys for unclear definitions and conflating child-on-child induced distress with adult-on-child grooming.

2.2. Qualitative and Analytic Research

2.2.1. Studies on Internet and Computer Crime

NCIS: Project Trawler, 1999

This was a study commenced by the National Criminal Intelligence Service (NCIS) in 1996 and was designed to inform the Home Office and police about the extent of "computer crime". There were two versions, one for law enforcement and the other which was published on the web but appears to be no longer available there. A copy is being supplied to NAO. The basic methodology consisted of a small team of researchers asking a variety of law enforcement and academic specialists for their views and marrying these up with statistics and other surveys then available. There were also seminars. *Trawler* is now largely of historic interest but it to the setting up of National High Tech Crime Unit (NHCTU) which existed between 2001 and 2006.

Home Office: Future of Netcrime Now 2004⁵⁴

This was a study carried out by the Home Office Research, Development and Statistics Directorate. It used a Delphi technique, essentially the use of structured questioning of a panel of experts drawn from government, law enforcement, regulation, industry and academia. The panelists did not know at the time who the other participants were. The questioning took place in three “rounds” in order to refine the answers. The study provides a useful review of the issues, but the recommendations are quite generalized. There is no indication that any specific public policy initiatives flowed from it

House of Lords Science and Technology Committee: Personal Internet Security⁵⁵

This was a Select Committee Report published in August 2007 and which received a large number of submissions. It does not set out to provide a formal analysis but the breadth of its coverage and the quality of some of the contributions means that it is worth reading. The Committee took on a very broad remit. The Report deals with the Internet structurally in terms of technical infrastructure, governance, and social/commercial institutions. As a result of this concentration on how the Internet “works”, it become easier to see where responsibilities for safety might lie – with individuals, with content providers, with suppliers of specialist infrastructure software (for example for web-servers, or “root” systems, or web-browsers) with ISPs, with governments. This is a useful antidote to those who complain about phenomena which they seek to blame generally on “the Internet” or on the companies that most immediately delivery internet services into the home.

The following are passages particularly worth consulting:

Para 2.43: “We recommend that the Government establish a cross-departmental group, bringing in experts from

⁵⁴ <http://www.homeoffice.gov.uk/rds/pdfs04/rdsolr6204.pdf>;

<http://www.homeoffice.gov.uk/rds/pdfs04/rdsolr6304.pdf>

⁵⁵ <http://www.parliament.the-stationery-office.com/pa/ld200607/ldselect/ldsctech/165/16502.htm>

industry and academia, to develop a more co-ordinated approach to data collection in future. This should include a **classification scheme for recording the incidence of all forms of e-crime**. Such a scheme should cover not just Internet specific crimes, such as Distributed Denial of Service attacks, but also e-enabled crimes—that is to say, traditional crimes committed

Para 3.9 ff This contains an analysis of the **efficacy of content filtering**, a possible remedy considered in more detail at page 98.

Para 3.20 ff considers **where responsibility for Internet security** should lie. The section concludes at para 3.34: “The current emphasis of Government and policy-makers upon enduser responsibility for security bears little relation either to the capabilities of many individuals or to the changing nature of the technology and the risk. It is time for Government to develop a more holistic understanding of the distributed responsibility for personal Internet security. This may well require reduced adherence to the “end-to-end principle”, in such a way as to reflect the reality of the mass market in Internet services.”

Section 5 deals with the **business use of the Internet**. It says: “...once individuals have made personal information available online, whether by sending an email, or using a search engine, or opening an online bank account, they no longer have direct control over the uses to which that information is put.... It would therefore seem to be incumbent on businesses operating online to protect their customers’ security and safety by ensuring that the information they hold is not lost. But as the Foundation for Information Policy Research noted, “Security failures are often due to misplaced incentives; when the people guarding a system are not the people who suffer when it fails, then one may expect less than the socially optimum level of diligence” (p 209). There is currently no direct commercial incentive for businesses to make the security of private individuals a high priority, given that it is those individuals who typically bear the losses resulting from security breaches.

Of **phishing** the Report says: (para 5.10 ff): The key point about phishing is that it works by means of social engineering—victims are persuaded to go to a fraudulent

site, on which they themselves enter their account details and other personal information. No malware needs to be involved, and standard technical measures such as antivirus software are of no use It follows that action by the companies whose customers are targeted and whose websites are spoofed by the phishers is essential to limit the threat to e-commerce. A key measure is the rapid closing down of phishing sites.

Para 5.42 ff: There is consideration of how to enforce the **current law that protects the security of personal data online** – the ICO, the FSA, and OFT. Since the Report was written the ICO has some increased powers

Paras 5.54 and 5.55 make the following recommendation: “We further believe that a **data security breach notification law** would be among the most important advances that the United Kingdom could make in promoting personal Internet security. We recommend that the Government, without waiting for action at European Commission level, accept the principle of such a law, and begin consultation on its scope as a matter of urgency. We recommend that a data security breach notification law should incorporate the following key elements: • Workable definitions of data security breaches, covering both a threshold for the sensitivity of the data lost, and criteria for the accessibility of that data; • A mandatory and uniform central reporting system; • Clear rules on form and content of notification letters, which must state clearly the nature of the breach and provide advice on the steps that individuals should take to deal with it.

Section 6 deals with individual use of the Internet and draws a **distinction between “awareness” and “knowledge”**; the first is about the existence of threats, the second about how to deal with them. It draws attention to research which casts doubt on the ability of some users properly to use available security facilities.

At para 6.16 there is **commentary on sources of information and advice**. The Report says of Government activity: “ There is thus a contradiction in the Government’s position. On the one hand they are rightly conscious of the need to provide a single, integrated source of information and advice on Internet security—Vernon Coaker described coordination of information as

“something we need to become smarter at” But at the same time the sources of information are diverse and overlapping”. It goes on to list some of these overlaps. (And this literature review carries out the same exercise though more extensively at page 102) . The section concludes with the following recommendation: “ The Government-sponsored Get Safe Online website already provides useful information and practical advice to Internet users, but its impact is undermined by the multiplication of other overlapping websites. We recommend that the Government provide more explicit high-level political support to the Get Safe Online initiative and make every effort to recruit additional private sector sponsors. If necessary, the site should be re-launched as a single Internet security “portal”, providing access not only to the site itself but acting as a focus and entry-point for other related projects.”. There are also recommendations for a “kite mark” scheme for content control software and that the DCSF promote a project to educate the adult population in particular parents, in online security and safety.

Para 7.20 ff considers **crime reporting**. It concludes: “We recommend that the Government, in partnership with the Association of Chief Police Officers and the Serious Organised Crime Agency, develop a unified, web-based reporting system for e-crime. The public face of this system should be a website designed to facilitate public and business reporting of incidents. The back-end software should have the capacity to collect and collate reports of ecrime, identify patterns, and generate data on the incidence of criminality. The website could also serve as a portal to other more specialised sites, for instance on online child abuse or identity theft. It would be an invaluable source of information for both law enforcement and researchers.” (Since this Report was written the Government has announced the setting up of the National Fraud Reporting Centre. However this presumably has the remit of “fraud” in general – see pages 18 and 115).

ENISA: Security, Economics and the Internal Market⁵⁶

This is a Report commissioned by ENISA, the European Network and Information Security Agency in 2007 and published in 2008. The work was carried out by some Cambridge computer security specialists and there is some overlap with the recommendations made by the House of Lords. (Some of the Cambridge team advised the Lords and gave evidence to the Select Committee.) This Report too recommends a security breach notification law, that the Commission or the European Central Bank regulate to ensure the publication of robust loss statistics for electronic crime and also asks that ENISA collects and publishes data about the quantity of spam and other bad traffic emitted by European ISPs. (In fact spam data is available from some anti-spam vendors – see page 66.)

2.2.2. Studies about Children Online

There are a number of generic problems of carrying out studies of the behaviour of children and children in their use of the online world. These include:

- Obtaining age-appropriate informed consent for the questioning
- Getting children to respond to questions and checking the veracity and integrity of what they say
- Problems of defining a “balanced” sample as issues such as stability of home life, the level of education and the wealth of parent(s) may be important
- Dealing with loose expressions such as “worry”, “upset”, “distress”
- The particular problems of asking about sex

There are also specific researcher ethics: You can’t put subjects into a situation where there is a possibility of causing them harm – but that means that a number of important questions remain unanswered, such as the extent of long-term harm a child may face when confronted with sexual images or having to cope with an

⁵⁶ http://www.enisa.europa.eu/doc/pdf/report_sec_econ_&_int_mark_20080131.pdf

adult perpetrator. Some of these issues are discussed at greater length in the EU Kids Online *Best Practice Research Guide*⁵⁷

In addition, Livingstone and colleagues say: "... this field encounters a range of theoretical, methodological and political difficulties in researching possible harms associated with media content. This is largely because different academic disciplines approach questions of media harm very differently. Typically, psychologists focus on evidence of harm to the emotions, beliefs, attitudes or social behaviours of individuals, preferring explicit measurement tools and, to isolate causation, experimental methods. Sociological and cultural researchers are generally critical of such approaches since they neglect the complex contextual factors that give meaning and shape actions in everyday life, potentially rendering experimental findings not generalisable to everyday life contexts. Both sides in this debate would agree that, in various respects, the evidence base is patchy and inconsistent and, for both practical and ethical reasons, some key questions remain difficult to research"⁵⁸

Byron⁵⁹ makes some further points:

- Research becomes quickly out of date and cannot move at the pace of technological change – a particular issue in the context of how long it can take to publish academic works.
- It is difficult to study long-term implications because the technology is often so new and use is changing.
- Much of the research is unhelpful for policy makers as it is more common to identify problems with the research than truly evaluate its implications.
- Much of the research (particularly within the experimental studies tradition) comes out of the States where the cultural context and concerns may be different.

Livingstone: UK Children Go Online⁶⁰

⁵⁷ Available from <http://www.eukidsonline.net/>

⁵⁸ Comment in <http://www.ofcom.org.uk/research/telecoms/reports/byron/annex6.pdf>

⁵⁹ <http://www.dcsf.gov.uk/byronreview/pdfs/Final%20Report%20Bookmarked.pdf>

This Report was referred to earlier for its base statistics (see page 39). This is what it has to say in terms of “softer” findings:

- Findings show that the internet has become a key information resource to support school work but that, despite their being widely identified as ‘experts’, ‘the internet generation’, children continue to struggle with the internet. A range of online competences were explored, from acquisition of specific skills to broader questions of critical literacy (e.g. evaluation of the trustworthiness and reliability of websites). Internet literacy emerges as an important player in the balance, struck differently in different households, between online opportunities and risks.
- Parents were found to be highly ambivalent regarding the internet, introducing it at home to support their child’s education, but then anxious about the accompanying risks. Their expertise was found to lag behind that of their children, resulting in a series of misunderstandings which affect parental support for and regulation of children’s internet use. Several project outputs analysed the complex relations between parental and child expertise and family dynamics in the home.
- Generally, parents seem to underestimate the risks their children experience online. On the other hand, it appears that children underestimate the rules and regulatory practices their parents attempt to implement. Parental anxieties may contribute to making domestic regulation ineffective, while children’s enthusiasm for the internet (and for maintaining their online privacy) results in some risky behaviours. The challenge for policy intervention is considerable, and several dissemination activities and project outputs have been concerned to develop ways forward with policy makers, industry representatives, police, government

⁶⁰ <http://www.lse.ac.uk/collections/children-go-online/End%20of%20Award%20Report,%20UK%20Children%20Go%20Online,%20Sonia%20Livingston.pdf>

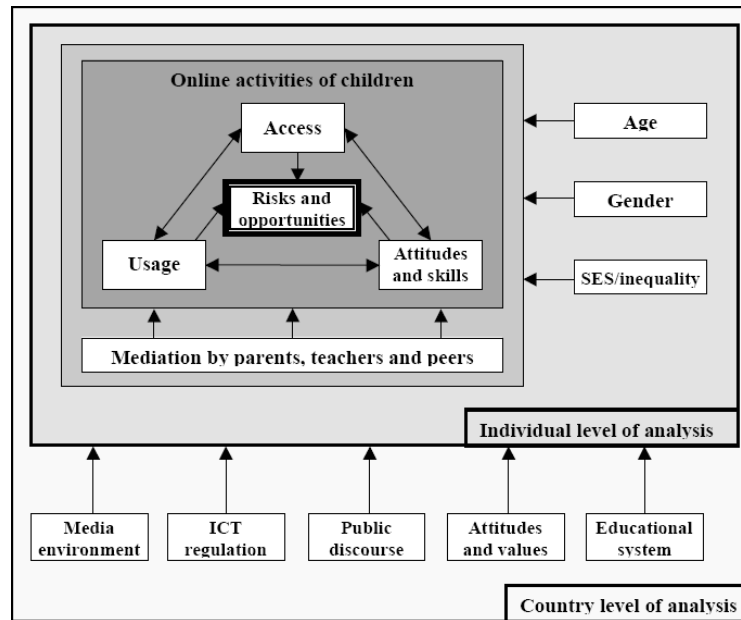
departments (including the Department for Education and Skills and the Home Office), regulators (e.g. Ofcom), children's charities and parenting groups.

- Young people are primarily excited by the internet as a communication medium, and they relish making skilful choices about communication, comparing email/instant messenger/text etc in terms of intimacy, embarrassment, privacy and cost, even preferring mediated to face-to-face communication. Most online communication is with local friends and they show little interest in contacting strangers. Despite popular expectation, the research did not find that online communication particularly encourages online participation in civic or public spheres. Indeed, an emergent theme of the project was young people's disaffection not only with political participation in general but with the hope the internet could change things. Rather, they were sceptical of the online invitation to 'have your say', leaving such participation to those already interested in, rather than drawing in those new to, political or civic concerns.

EU Kids Online⁶¹

EU Kids Online is a follow-up to the UK study using similar techniques but, as the name suggests, gathering information across Europe. The chart below shows the scope of the research, which is on-going.

⁶¹ <http://www.eukidsonline.net/>



Byron: Safer Children in a Digital World⁶²

This 2008 Report is the result of a commission from the Prime Minister to review the risks children face from the Internet and video games. It was written by a clinical psychologist who had achieved prominence via various television appearances.

The research approach uses the same framework as Livingstone. However there is relatively little in the form of new original research from proper balanced samples.⁶³ There was a Call for Evidence from children which received 350 responses from children between 5 and 18, all of whom were self-selected. There were focus groups involving 48 parents and 42 children and “talking” with Children’s Panels at CEOP and DCSF. There was then a further Call for Evidence which received over 300 responses from key industry, third sector and individual stakeholders and further meetings and an interim conference.

⁶² <http://www.dcsf.gov.uk/byronreview/pdfs/Final%20Report%20Bookmarked.pdf>

⁶³ The research methodology is described at

<http://www.dcsf.gov.uk/byronreview/pdfs/Focus%20Group%20Research%20Final%20Report.pdf>

However there is a useful literature review from Professor David Buckingham⁶⁴ and the process also prompted the publication of a separate literature review by Ofcom by Livingstone and colleagues at the LSE⁶⁵

Byron recommended the setting up of UK Council for Child Internet Safety – UKCCIS (this has since taken place⁶⁶).

Byron’s specific recommendations in relation to the Internet are:

- That through the Council, the relevant industries should develop an independently monitored voluntary code of practice on the moderation of user generated content, including making specific commitments on take-down times.
- That through the Council, industry should ensure that computers sold for use in the home in the UK should have Kite-marked parental control software which takes parents through clear prompts and explanations to help set it up and that ISPs offer and advertise this prominently when users set up their connection.
- That through the Council, search providers should agree to make it obvious to users what level of search is on (e.g. safe or moderate) and give users the option to ‘lock it’ on and that every search engine have a clear link to child safety information and safe search settings on the front page of their website – this is particularly important as most parents are comfortable using search functions.
- That through the Council, the relevant industries should work with Government and the third sector to support vulnerable children and young people, especially in signposting users to support services when they discuss harmful behaviours, improving the skills of moderators and raising awareness of online risks with those who work with vulnerable children. That the advertising industries take steps to

64

<http://www.dcsf.gov.uk/byronreview/pdfs/Buckingham%20Impact%20of%20Media%20Literature%20Review%20for%20the%20Byron%20Review.pdf>

⁶⁵ <http://www.ofcom.org.uk/research/telecoms/reports/byron/annex6.pdf>

⁶⁶ <http://www.dcsf.gov.uk/ukccis/>

‘futureproof’ the current system for regulating advertising to take account of new forms of online advertising which are currently out of remit and that Government reviews progress in this area in a year’s time when it has the conclusions of the assessment of the impact of the commercial world on children’s wellbeing.

- That the advertising industry works with media owners to raise awareness amongst advertisers of their obligations under the CAP Code to advertise responsibly to those under 18 on the internet and that the Council keeps this under review.

Useful sections within Byron include commentaries on: Sexually explicit content at para 3.32 esp 3.34; Commercial content at para 3.42; Stranger danger at para 3.50; Bullying at para 3.60; Harmful sites, incl suicide and hate at para 3.68; Age verification schemes at para 4.84; Content labelling at para 4.90; and public awareness programs at paras 5.43, 5.65. and 5.69.

IPPR: Behind the Screen – hidden life of youth online ⁶⁷

This 2007 Report is based on desk research and three “deliberative workshops” each consisting of 12 participants drawn from three areas in Inner London. Despite claims that they were a broadly demographically representative sample of the population and were recruited to include the full range of socio-economic groups, it is difficult to see how this can be achieved with only 36 London-dwelling individuals. As a result, the Report is probably better read as the opinions of the authors based on their readings. Their observations are as follows:

⁶⁷ http://www.ippr.org/members/download.asp?f=/ecomm/files/behind_the_screen_20.pdf - requires IPPR login

•Young people have contradictory attitudes towards the internet Young people describe many aspects of internet use as both positive and negative. For instance, while they describe the increased opportunity to socialise with friends as a benefit, they also express concern at the ‘addictive’ nature of the internet. The sum of time spent online, and the importance placed on ‘constant connectivity’ has implications for young people’s well-being and psychosocial

development, theories of which emphasise the need to spend time alone.

•Attitudes to privacy and safety are extremely contradictory Young people experience a tension between a strong dislike of strangers looking at their social networking profiles, and a sense that a major benefit of having a social networking site (SNS) profile is the opportunity to self-advertise. Young people emphasise the need to add photos and detail on their online profiles in order that people will want to become their friends. This process is regularly referred to as ‘selfadvertising’. They also reject the notion of making their profile private, as this would stop it being viewed widely.

•Attitudes to meeting new people are contradictory For example, young people are well aware of ‘stranger danger’, and tend to use the internet to socialise with people they already know. There are also strong norms against using the internet to meet new people. Nonetheless, young people do use the internet to communicate with ‘friends of friends’ – people with whom they have some connection, no matter how tenuous – for example, someone who was linked through a social networking site or copied into the same chain email. When young people do meet up with ‘friends of friends’ they have met online, they have a number of mechanisms they employ in order to ensure their safety. For instance, they place more trust in a webcam than a photo in establishing identity, as there is recognition that photos can be fake. They

also tend to meet people with a group of friends rather than alone.

Cyberbullying is not a recognised concept

Young people do not tend to use the term 'cyberbullying', and there are strong norms towards 'seeing the joke' where online behaviour is concerned. The context of offline relationships is crucial in deciding whether certain actions online are acceptable or not - for instance, posting 'joke' or embarrassing photos or videos of friends or acquaintances online. The particular implications of online exposure are not significant for young people. They often do not distinguish between doing something embarrassing or harmful to someone and putting an image of this online.

The authors conclude:

First, young people conceptualise risk in terms of immediate, quantifiable consequences of behaviour. Young people's concepts of risk are largely formed through the stories in the news media and were negotiated in terms of the likelihood of a negative consequence, including being caught. So, for example, where activities such as plagiarism, activities equating to adult definitions of 'cyberbullying' and lax attitudes to privacy are concerned, young people feel relatively free from consequence, and therefore do not consider such activities to be 'risky'.

Second, young people do not reflect on their online behaviour. This extends to young people's lack of awareness of the implications of online exposure of themselves and others, a limited concept of the audience who may be viewing their activities online, and the extent to which they are willing to take information accessed online at face value.

Overall, these findings suggest that young people's technical expertise can often exceed their understanding. This is the gap which policy must bridge to ensure that young people are not needlessly putting themselves at risk online and instead can get the most out of what the internet has to offer.

CEOP: Online Social Networks ⁶⁸

Margaret Brennan, 2006. This is described as a “preliminary” report and is based on a series of 16 “stakeholder workshops” held over 4 days. There were both Youth and Adult stakeholders. The observations and conclusions are in line with others. The Report ends, honestly enough: “At present, much of our knowledge on the topic of safeguarding children in social networks is anecdotal rather than empirically-based. Safeguarding interventions will only be effective if they are grounded in a real and evidenced knowledge base - this requires further research to fill existing knowledge gaps on risk factors and possible interventions in social networking environments.”

Eurobarometer. : Towards a safer use of the Internet in the EU - a parent’s perspective⁶⁹

This is work commissioned by the EU Safer Internet Program in late 2008. It was conducted by Gallup and covered the use of the Internet and mobile phones by children. The survey scope was limited to *parents* as opposed to children. A total of 12, 750 parents from 27 EU countries was randomly selected. Most interviews were by telephone.

The quantitative aspects of the Report are given above at page 42. Below are some of the findings from the more qualitative work:

⁶⁸ http://www.ceop.gov.uk/downloads/documents/socialnetwork_serv_report_221206.pdf

⁶⁹ http://ec.europa.eu/information_society/activities/sip/eurobarometer/index_en.htm

Concerns and awareness about online risks

The biggest risk in parents' eyes (65%) was that their child might see sexually or violently explicit images on the Internet: 45% were *very* worried.

In terms of inappropriate contact, parents were most worried that their child could become a victim of online grooming (60%); other concerns were that their child could be bullied online by other children (54%) or bullied by others over a mobile phone link (49%).

Parents were the least worried that their child might reveal personal or private information when using the Internet: only a quarter said they were *very* worried and 21% were *rather* worried.

Parents in France, Spain, Portugal, Greece and Cyprus worried the most that their child might see inappropriate content, make contact with someone intent on grooming or bullying, or reveal personal information. Parents in Denmark, Sweden and Slovakia had the least concern there.

Parents who did not use the Internet themselves, but who said that their child did use it, most frequently answered that they were *very worried* about the risks faced by their child when using the Internet and mobile phones.

Parents answering a question about their 6-10 year-old or their 11-14 year-old more frequently said they were *very worried* about the risks their child faced when using the Internet and mobile phones.

Offering assistance to children in case of problems

Only a minority of the respondents said that when their child asked for their help with an Internet-related problem, this was due to: contact online by a stranger (4%), harassment (4%) or bullying online (3%), or the existence of sexually or violently explicit images on the Internet (4%).

Almost three out of 10 Dutch parents (28%) and a quarter of the parents in the UK (24%) said that, when their child asked for their help, this was because they had been contacted by a stranger, were bullied or harassed online or saw violently or sexually explicit images online.

Older children, who asked their parents for help, more often did so for any of the reasons listed above (e.g. 7% of the 15-17 year-olds asked their parents for help because they were harassed online compared to 1% of the 6-10 year-olds).

Strategies for parental supervision when children use the Internet

Three-quarters of parents – with a child who accessed the Internet at home – said they always or very frequently talked with their son or daughter about what they had been doing online. A majority of the parents (61%) took care that they – always or very frequently – stayed nearby when their child used the Internet, while one-third said that they sat next to their child when they used the Internet.

Parents in almost all Member States were the least likely to regularly check whether their child had a profile on a social networking site (30%) or the messages in their child's email or IM account (24%).

Parents in the UK and some southern European countries – Portugal, Italy and Spain – were more likely to regularly supervise their child when using the Internet (e.g. stay nearby or sit next to their child) and to check what their child had done online (e.g. check the history file or e-mail account).

Parents in Lithuania and Estonia, on the other hand, were each time among the most likely to answer that they never supervised or checked their child's Internet-related activities.

The 15-17 year-olds were subject to less parental supervision than the 11-14 year-olds and the 6-10 year-olds, but this reduction was more noticeable in the supervision of children using the Internet than for the monitoring of children's online activities (e.g. checking the history file or e-mail).

Half of the parents participating in this survey answered that they had installed filtering software on the computer that their child used at home. Monitoring software was not as popular, but was still used by almost four out of 10 parents (37%).

Parents in all of the EU27 Member States most often thought of the police when asked how they would report illegal or harmful content seen on the Internet – 92% gave this response. Four out of 10 parents (38%) would report such content to a hotline set up for this purpose and one-third mentioned non-profit or other associations.

Parents who did not use the Internet were more likely not to know how they would report illegal or harmful content seen on the Internet. For example, almost one-fifth of the parents who did not use the Internet did not know they could report illegal content to a hotline set up for this purpose compared to 12% of the parents who did use the Internet.

Sources for information and advice about safer use of the Internet

Family and friends were the most popular source of information or advice for parents about monitoring and filtering tools and safe use of the Internet: 71% of parents had turned to a friend or family member to discuss Internet safety issues.

Four out of 10 parents had browsed the Internet and found information or advice about safer Internet on various websites, and a similar proportion (36%)

counted on Internet service providers (ISPs) to get such information.

Berkman: Enhancing Child Safety and Online Technologies - Internet Safety Technical Task Force⁷⁰

This is a 2008 US report commissioned by 50 attorneys-general from the 50 states of the union. It produced a Literature Review of relevant research in the field of youth online safety in the United States, which documents what is known and what remains to be studied about the issue and a report from its Technology Advisory Board, reviewing the 40 technologies submitted to the Task Force.

An interesting feature of the Report is its critique of research methodologies and the way in which statistics may be abused. “The methodology of a study is its most important quality. The size of a sample population matters less than how the population was sampled in relation to the questions being asked. The questions that qualitative studies can address differ from those that can be addressed quantitatively, but both are equally valid and important. ...Presenting statistical findings is difficult, because those who are unfamiliar with quantitative methodology may misinterpret the data and read more deeply into the claims than the data supports. For example, correlation is not the same as causation, and when two variables are correlated, the data cannot tell you whether one causes the other or whether an additional mediating variable that affects both is involved. In presenting the findings of different studies, the Literature Review tries also to provide a roadmap for understanding what these studies mean and also includes some background”

The study looks at “sexual solicitation and internet-initiated offline encounters”, “online harassment” and “problematic content”. Among the findings:

⁷⁰ <http://cyber.law.harvard.edu/pubrelease/isttf/>

- Bullying and harassment, most often by peers, are the most frequent threats that minors face, both online and offline.
- Much of the research based on law-enforcement cases involving Internet-related child exploitation predated the rise of social networks. This research found that cases typically involved post-pubescent youth who were aware that they were meeting an adult male for the purpose of engaging in sexual activity.
- Youth report sexual solicitation of minors by minors more frequently, but these incidents, too, are understudied
- The Internet increases the availability of harmful, problematic and illegal content, but does not always increase minors' exposure. Unwanted exposure to pornography does occur online, but those most likely to be exposed are those seeking it out, such as older male minors.
- Minors are not equally at risk online. Those who are most at risk often engage in risky behaviour and have difficulties in other parts of their lives. The psychosocial makeup of and family dynamics surrounding particular minors are better predictors of risk than the use of specific media or technologies.
- Although much is known about these issues, many areas still require further research. For example, too little is known about the interplay among risks and the role that minors themselves play in contributing to unsafe environments.

2.2.3. Exploitation of children in a retail Internet situation

In contrast to the position in the United States where there is specific legislation to protect children, the Children's Online Privacy Protection Act, 1998 ("COPPA") and where there is a significant amount of literature, this topic has not received much

attention in the United Kingdom. The National Union of Teachers (NUT) makes a passing mention in its *Growing Up in a Material World* Charter of 2007⁷¹. There is further mention in Sue Palmer's *Toxic Childhood*⁷². In the US there are a number of dedicated websites such as <http://dads.e-actionmax.com/showalert.asp?aaid=522> and <http://www.commondreams.org/>. A useful guide to the US situation is provided by Privacy Rights at <http://www.privacyrights.org/fs/fs21-children.htm>.

Byron makes a brief comment at para 3.42 of her Report:⁷³ “There are questions relating to children’s vulnerability to persuasion or exploitation not just from advertising but from content more generally. The small amount of research that has been done shows that young people seem very good at ignoring advertising (Chester and Montgomery, 2007) . They often show considerable cynicism about it (Buckingham, 1993) and are critical of mainstream advertising (Seiter, 2005). However, another study found that children tend to believe content on sites that include advertising (Eastin, Greenberg and Hofschire, 2006) and another, that children are confused by the blurring of advertising and content (European Research into Consumer Affairs report, 2001).”

In December 2007 the Government announced in the Children’s Plan that it will assess the impact of advertising, marketing and other commercial activity on children and their childhood. Leading academics will examine all the available evidence about changes in the commercial environment (and in particular whether there is any evidence that developments impact on children’s wellbeing) with the aim of building a new consensus on the nature and extent of the impact of commercialisation in the round. Their assessment will also look at the benefits children gain from commercial engagement (including the economic contribution of industries and sectors that provide products to young people). The end-of-year report for the Children’s Plan⁷⁴ shows that the commercialization aspect has not yet been completed.

⁷¹ <http://www.teachers.org.uk/resources/pdf/MaterialWorld24pp.pdf>

⁷² Orion, 2007

⁷³ <http://www.dcsf.gov.uk/byronreview/pdfs/Final%20Report%20Bookmarked.pdf>

⁷⁴ <http://www.dcsf.gov.uk/oneyearon/ae/uploads/documents/flagship.pdf>, published in December 2008

2.2.4. Miscellaneous Further Articles worth noting

Phishing as a Tragedy⁷⁵

This paper deals with the economics of phishing and in contrast to commonly-held views concludes that it is a low skill-low rewards business and that many of the oft-quoted statistics are exaggerated. The authors say: "... data showing that phishing losses are huge crumble upon inspection. We review the main surveys and technical studies of phishing rate Most of the data are from victim surveys. While surveys are a very valuable source of data, crime researchers have known for some time that victim surveys have several sources of bias:

- Selection bias (*i.e.* failure to contact a representative sample of the overall population)
- Refusal rate (*i.e.* rate at which contacted population refuse to respond to the survey)
- Telescoping (*i.e.* tendency of respondents to "throw in" incidents that do not fall within the time frame of the survey)
- Forgetting (*i.e.* tendency to omit crimes that do fall in the time frame or have been forgotten)
- Exaggeration of losses (*i.e.* tendency of victims to overstate rather than understate the magnitude of the wrong they have suffered).
- Almost all of the surveys take the average reported loss per victim and scale this loss to the entire population. It cannot be emphasized strongly enough that a few victims who claim extravagant losses can bias the *average* numbers greatly upward (the same is not true of the median)".

Symantec: Web-based attacks ⁷⁶

⁷⁵ <http://research.microsoft.com/apps/pubs/?id=74159>

⁷⁶ http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_web_based_attacks_03-2009.en-us.pdf

This white paper describes current trends in web-based attacks and makes the following predictions:

Top Web Threat Trends for 2008	
1. Drive-by downloads from mainstream Web sites are increasing	
2. Attacks are heavily obfuscated and dynamically changing making traditional antivirus solutions ineffective	
3. Attacks are targeting browser plug-ins instead of only the browser itself	
4. Misleading applications infecting users are increasing	
5. SQL injection attacks are being used to infect mainstream Web sites	
6. Malvertisements are redirecting users to malicious Web sites	
7. Explosive growth in unique and targeted malwares samples	

MacAfee 2009 Threat Predictions⁷⁷

This anti-malware software publisher suggests the growth of fake financial transactions services, fake investment firms, fake legal services, and “mule recruitment” emails (where people are induced to take on part-time work as a “transaction fulfilment agent” which turns out to involve money-laundering. The report also deals with new technology-based threats.

⁷⁷ http://www.mcafee.com/us/local_content/reports/2009_threat_predictions_report.pdf;

3 Review of ‘counter-measures’

Counter-measures to prevent or limit the effects of “Internet Crime” can be applied by consumers/potential victims, by commercial companies as a service, by Internet Services Providers as a service, by NGOs as a service, and by Government. There are specific technical measures, awareness/educational programmes, and victim response programmes. In addition Governments can resource their law enforcement agencies, though this route is beyond the remit of the present study.

3.1. Technical preventative measures that can be applied by potential victims

3.1.1. Patching and updating software and applications

Operating Systems and computer programs often turn out to have security weaknesses that only appear after they have been released. In response software houses issue free updates to registered users. The only cost to the consumer is the time taken to accept and enable the updates.

3.1.2. Anti-virus, anti-trojan, anti-malware software

Software which regularly scans the contents of computers as well as newly received input is widely available. Some basic software is available at no cost and is adequate to protect consumers; others are offered for sale on a low-cost subscription basis. The software carries a large database of the signatures of known viruses, Trojans and other malware; the database is usually updated daily. In addition to stopping viruses which might destroy or corrupt a computer’s contents, the software will also often detect attempts at installing remote control software which might be used in one or more stages in phishing, attempts at unauthorised access and the creation of botnets.

3.1.3. Firewalls

A firewall is, at its simplest, a program which limits access to a computer across a network, including the Internet. A firewall program will monitor traffic both into and out of a computer and alert the user to apparent unauthorised usage. A basic software firewall is included in Windows XP and Vista. More sophisticated

packages are available. For SMEs it is also possible to buy a hardware-based firewall, which in essence is a separate stand-alone specialist computer which monitors traffic into and from the corporate network

3.1.4. Anti-spam services

These services work in a number of ways. They can be fed with “black-lists” of locations and email addresses from which spam is known to emanate so that they can be blocked. They can also work on “signatures” which might relate to trigger words or combinations of words. From the consumer’s perspective, anti-spam facilities are most conveniently provided by Internet Service Providers, sometimes for a small additional fee. It is however possible to buy products where the spam is excluded by software installed on the user’s own PC. Details of how blocklists work can be found at the Spamhaus website.⁷⁸

3.1.5. Anti-phishing services

As with anti-spam facilities, these services work in a number of ways. They can be fed with “black-lists” of locations and email addresses from which phishing attempts are known to emanate so that they can be blocked. They can also work on “signatures” which might relate to trigger words or combinations of words. Microsoft provides basic anti-phishing facilities within more recent versions of its free browser, Internet Explorer. Some Internet Service Providers, sometimes also offer services for a small additional fee.

3.1.6. Subscription-based external malware, firewall and intrusion detection services

Small and larger companies can buy services from specialist third parties. All their Internet traffic is routed via these services, which monitor for, and react to, malware and other untoward activity. The advantage is that knowledge of threats is likely to be more immediately up-to-date and clients do not have to keep specialist security staff.

⁷⁸ http://www.spamhaus.org/dnsbl_function.html

3.1.7. Content Filtering Programs

These are programs which filter material arriving on a computer on the basis of single words, combinations of words, black-lists of known “troublesome” sites and in some instances claim to be able to scan photographic images to assess if they are pornographic. The websites <http://www.internet-filter-review.toptenreviews.com/>; <http://filteringfacts.org/filter-reviews/filter-tests/> and <http://www.getnetwise.org/> list a number of the most popular programs. More sophisticated analyses can be found at: *Calculating Error Rates for Filtering Software*, Resnick, Hansen and Richardson Communications of the ACM Volume 47, Issue 9 (September 2004) <http://www.si.umich.edu/~presnick/healthfiltering/CACM.pdf>. The EU Safer Internet Program Filtering Report 2008 is located at http://ec.europa.eu/information_society/activities/sip/projects/targeted/filtering/sip_bench/index_en.htm#results2008 http://ec.europa.eu/information_society/activities/sip/docs/project_reports/sip_bench_2008_synthesis_report_en.pdf.

Another form of filtering is based on **web-labelling schemes**, which are considered below. Popular web-browsers such as Microsoft Internet Explorer have in-built facilities to recognise and react to web-labelling schemes.

The general view is that content-filtering programs can offer partial solutions but can both under-block (let troublesome material through) and over-block (prevent desirable material from being seen). Many of the packages are designed to be used by parents who can, within limits, set their own criteria. A frequently asserted concern is that slightly older children may be quite able to adjust the filtering themselves and indeed possess greater computer skills than their parents.

The House of Lords considered web-filtering at para 3.9 of its *Personal Internet Security Report*⁷⁹. Byron recommends a kite-mark system for filtering software at para 4.71 of her Report⁸⁰

⁷⁹ <http://www.parliament.the-stationery-office.com/pa/ld200607/ldselect/ldsctech/165/16502.htm>

⁸⁰ <http://www.dcsf.gov.uk/byronreview/pdfs/Final%20Report%20Bookmarked.pdf>

3.1.8. Web-labelling schemes

The idea behind this concept is that web-designers agree to “label” their own websites so as to give some idea of their content. The actual labels remain hidden to the ordinary viewer but are read by the browser software which then decides whether to display the results according to criteria set by the user. Microsoft Internet Explorer’s facilities can be seen by following Tools > Internet Options > Content. Obviously the user has to know that the facilities are there to be used – and the suspicion is that most do not. The most widely used scheme is called “ICRA” (Internet Content Rating Association) and is run by the Family Online Safety Institute.⁸¹ The main weakness is that its use by websites is entirely voluntary.

3.2. Technical preventative measures that can be applied by ISPs

3.2.1. AntiSpam

As we have seen ISPs can sometimes provide a more efficient service to customers than that available to consumers on their own machines. This can apply to malware detection, spam removal, anti-phishing detection and content filtering. The advantage is that the ISP may be able to use more sophisticated and more frequently updated detection algorithms. The disadvantage is that they may block harmless but desired email and web traffic. In those circumstances the intended recipient may not realise what has happened.

3.2.2. Content Filtering

Most UK ISPs receive information from the Internet Watch Foundation (IWF) about sites offering illegal material and filter web traffic based on the IWF list. This is described in more detail below.

⁸¹ <http://www.icra.org/>

3.3. NGO-provided facilities

3.3.1. Hotlines

Hotlines receive warnings from the public about sites and images which are believed to be illegal. The UK version, and it is a pioneer, is called the Internet Watch Foundation (IWF) - <http://www.iwf.org.uk/>. It is funded by the ISP industry but enjoys recognition from the Government, police and Crown Prosecution Service. IWF staff read the reports, which typically come in via a form provided on their website, and if they agree the material is illegal, the site or image is entered on to a list which is then provided to ISPs. The ISPs can use this as a basis of filtering. The BT version of this is called “Cleanfeed”. The list is also shared with a number of overseas hotlines. IWF only deals in material that is specifically illegal under UK law, which means child sexual and extreme pornographic material. It refuses action on material which is merely “disturbing”.

IWF is considered to be an example of co-regulation, a pragmatic solution to a problem which would otherwise result in many police enquiries of ISPs. There have been some minor criticisms, including how it determines the thresh-hold test for illegal material and the ways in which ISPs implement the black-list – sometimes whole sites have been blocked by individual ISPs when only one small part was thought to be illegal.

IWF offers very little in the way of general advice, as it regards this as outside its remit.⁸²

3.3.2. Age Verification Services

A further solution to controlling what children see that is sometimes discussed are services which verify a child’s age and use that as a means to deny access to unsuitable material. The topic is discussed at length (and in relation to mobile services and video games as well as the regular Internet) at:

http://ec.europa.eu/information_society/activities/sip/docs/pub_consult_age_rating_sns/reportageverification.pdf. One of the more convenient ways of establishing age at least for older children is via information that would have been supplied to a credit or debit card company.

⁸² <http://www.iwf.org.uk/public/page.2.htm>

3.3.3. Phishing Emails

Phishing emails can be reported to APACS via email:
reports@banksafeonline.org.uk.

3.4. Awareness and Educational Programs

There are a vast number of websites offering information and advice on Internet risks targeted both at adult consumers and children; very few are specifically aimed at older people. The websites are provided by charities, NGOs, individuals, trade associations and, to a limited extent, by government and law enforcement.

There is a great deal of overlap between the categories listed below. In addition, many of the websites cover topics of which Internet hazards are only one. Unless the sponsoring organisations are willing to furnish figures, it is extremely difficult to ascribe costs to individual initiatives; indeed it would not be surprising that some initiatives had not been costed at all.

The Government is in the course of rationalising all its consumer-orientated web services to remove duplications and provide a single portal via DirectGov, but this process is far from over. (source: John Suffolk, HMG Chief Information Officer)

In a number of instances representative examples are supplied, but the list is far from exhaustive:

3.4.1. General

Directgov:

http://www.direct.gov.uk/en/HomeAndCommunity/TechnologyInYourHome/InternetTechnologies/DG_10038607

GetsafeOnline: <http://www.getsafeonline.org/>

Internet Safety Zone: <http://www.internetsafetyzone.co.uk/>

Home Office Task Force Advice: These publications date from 2005: <http://police.homeoffice.gov.uk/operational-policing/crime-disorder/child-protection-taskforce#>;
<http://police.homeoffice.gov.uk/publications/operational-policing/moderation-document-final.pdf?view=Binary>;

<http://police.homeoffice.gov.uk/publications/operational-policing/search-and-advice-public.pdf?view=Binary>

National E-Crime prevention Centre: <http://www.necpc.org.uk/>
would-be umbrella organisation based at the University of
Wolverhampton but enjoying some police support

Ecrimeswales: <http://www.ecrimewales.com/> Welsh, but widely
admired within the police

Citizens Advice Bureau:
http://www.adviceguide.org.uk/i_fraud_on_the_internet.pdf

Symantec Cybercrime Advice:
<http://www.symantec.com/norton/cybercrime/index.jsp> (US-based
site which points to US sources of advice, provided by security
software vendor)

McAfee Advice:
<http://home.mcafee.com/AdviceCenter/Default.aspx> - provided by
security software vendor

Sophos Advice: <http://www.sophos.com/security/> provided by
security software vendor; covers much more than Internet crime

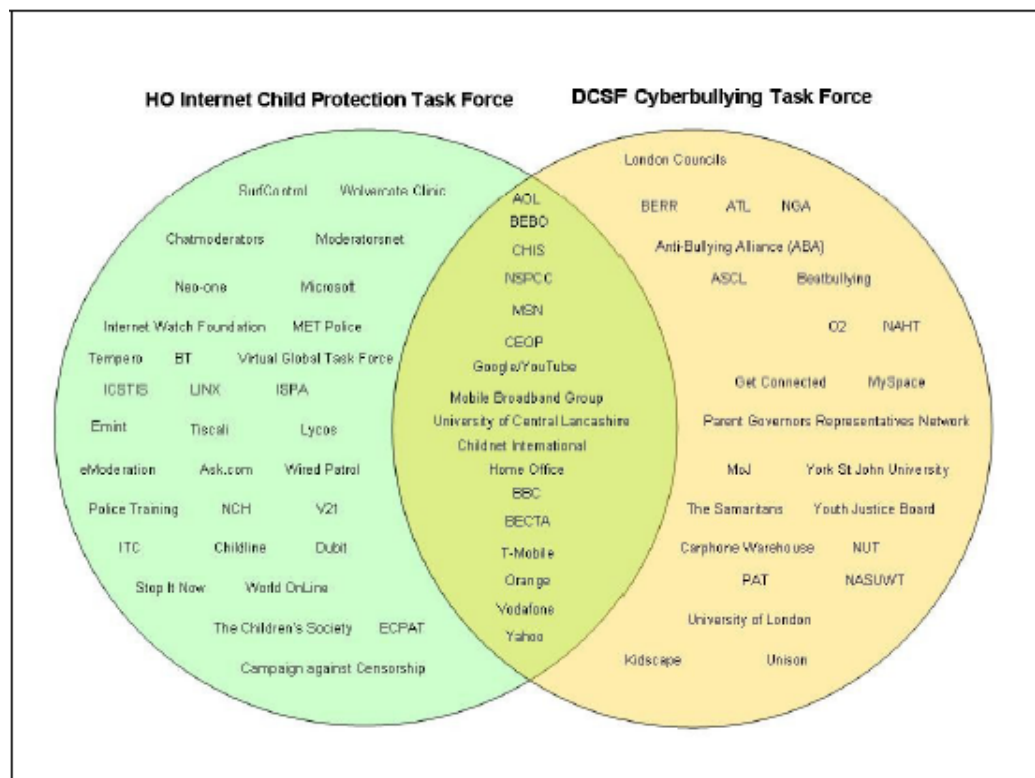
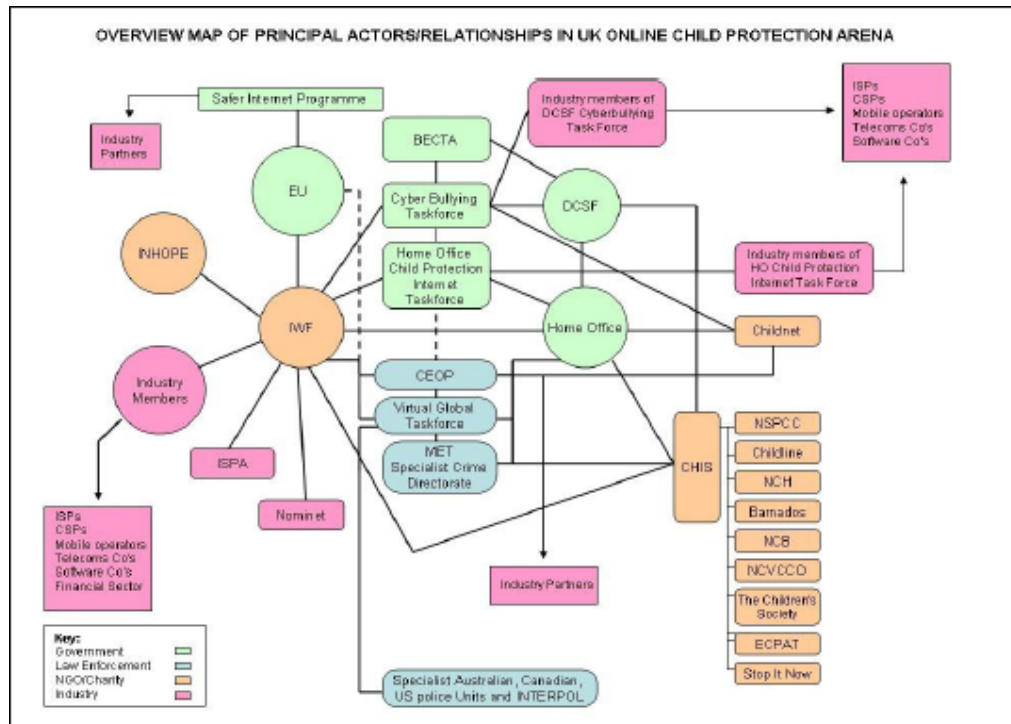
BanksafeOnline: <http://www.banksafeonline.org.uk/> mostly about
bank and card transactions

E-Victims: <http://www.e-victims.org/contact-us/> a would-be
umbrella service but so far very poorly funded.

3.4.2. Advice for Children

The best single guide to the very wide range of responses to protect children is supplied by EURIM its *Online Child Protection Report*⁸³ -. This provides an extensive list of the various UK agencies, charities, industrial bodies and umbrella groups. It covers “protecting children from adults”, “protecting children from adult content” and “protecting children from each other”. There are a number of extremely useful charts showing the extent of overlap and duplication of initiatives, eg

⁸³ www.eurim.org.uk/activities/childprotection/Online_Child_Protection_Report.doc



For the purposes of this Literature Review I won't repeat the contents of the EURIM Report. However it does rather raise the question of when UKCCIS (see page 83) set up in the wake of the Byron report is really necessary.

3.4.3. Advice for “Silver Surfers”

Age Concern:

http://www.ageconcern.org.uk/AgeConcern/Documents/FS33Crime_prevention_for_older_people.pdf This leaflet covers all kinds of crime as they affect older people; Internet crime appears indirectly via “Identity Theft”

Saga: <http://www.saga.co.uk/money/managingyourmoney/phishing-online-on-the-rise.asp>;
<http://www.saga.co.uk/money/gettingthebestdeal/safe-trading-on-ebay.asp>; <http://www.saga.co.uk/money/gettingthebestdeal/online-shopping.asp>

3.4.4. Fraud Advice

DirectGov:

http://www.direct.gov.uk/en/HomeAndCommunity/TechnologyInYourHome/InternetTechnologies/DG_10038621

Metropolitan Police:

<http://www.experian.co.uk/downloads/business/internetfraud.pdf>

New Business: <http://www.newbusiness.co.uk/articles/internet-advice/how-protect-against-online-fraud>

ShopSafeOnline: <http://www.shopsafeonline.org.uk/> This site is about credit card protection schemes

BankSafeOnline: <http://www.banksafeonline.org.uk/> This also allows for scams to be reported online and for advice to be requested in respect of suspect emails. Service provided by APACS.

BecardSmart: <http://www.becardsmart.org.uk/home/> (Visa, Mastercard and Apacs)

Paypal advice: <http://www.paypal.com/cgi-bin/webscr?cmd=p/gen/fraud-prevention-outside> relates specifically to the use of the PayPal service

3.4.5. Business Advice

Some of the advice available is more generally about “business crime” or “Cybercrime”. The following are samples which appear to cover Internet crime more specifically

Home Office: <http://www.homeoffice.gov.uk/crime-victims/reducing-crime/internet-crime/>;
http://www.homeoffice.gov.uk/documents/SME_Document.pdf

BERR general advice:
<http://www.berr.gov.uk/whatwedo/sectors/infosec/infosecadvice/resources/furtherhelp/page33312.html>

BERR Advice on Internet Auctions:
<http://www.berr.gov.uk/whatwedo/consumers/factsheets/page38202.html>

GetSafeOnline:
http://www.getsafeonline.org/nqcontent.cfm?a_id=1046

Metropolitan Police: <http://www.met.police.uk/business/>

Merseyside Police:
<http://www.merseyside.police.uk/html/crimeprevention/business/fraud/internet.htm>

Barclaycard (on card fraud):
http://www.barclaycardbusiness.co.uk/information_zone/security/managing_internet_fraud.html

Cyberfraud:
<http://www.cyberfraud.org.uk/home/whatiscybercrime.aspx>

Telecoms Advice:
http://www.telecomsAdvice.org.uk/features/e_crime_internet_crime_and_broadband_security_issues.htm

3.4.6. Advice from Police

The following are only examples; it will be seen that the quality varies considerably between different forces:

Metropolitan Police: <http://www.met.police.uk/computercrime/>

Essex Police: http://www.essex.police.uk/advice/v_int_01.php

Devon and Cornwall Police: <http://www.devon-cornwall.police.uk/v3/crime/online/index.htm>

Avon and Somerset Police:
http://www.avonandsomerset.police.uk/community_safety/internet_advice/

Cheshire Police:
<http://www.cheshire.police.uk/showcontent.php?pageid=790>

Norfolk Police:
<http://www.norfolk.police.uk/articleListing.cfm?catID=689>

Merseyside Police:
<http://www.merseyside.police.uk/html/crimeprevention/business/fraud/internet.htm> (in fact advice for online retailers)

Sussex Police:
http://www.sussex.police.uk/comp_crime/comp_crime.asp

City of London Police:
<http://www.cityoflondon.police.uk/CityPolice/Advice/ComputerSecurity/> But this is about corporate computer security and is big-business orientated;
<http://www.cityoflondon.police.uk/CityPolice/ECD/ScamsAdvice/emailscam.htm>;
<http://www.cityoflondon.police.uk/CityPolice/ECD/ScamsAdvice/IdentityTheft/>

3.4.7. Advice from ISPs

Many ISPs offer small amounts of advice about self-protection to their customers. The quality varies and for some ISPs the main drive seems to be to sell extra services. Again, these are simply examples:

BT Internet:
http://www.telecomsAdvice.org.uk/features/e_crime_internet_crime_and_broadband_security_issues.htm. Rather a lot of prompting to purchase an additional service called BT NetProtect

AOL: <http://daol.aol.com/security/>? Mostly prompts to but additional products – from McAfee. AOL is now owned by Carphone Warehouse

Sky Internet:

<http://www.sky.com/portal/site/skycom/securitycentre/article?contentid=3219010&catlist=3132510>

Carphone Warehouse/TalkTalk:

<http://www.carphonewarehouse.com/broadband/home-broadband>

Very perfunctory coverage; also:

<http://www.carphonewarehouse.com/support/advice-and-assistance/online-safety>

Virgin Internet:

<http://www.virginmedia.com/help/internetsecurity/tips/> General advice plus offer of PCGuard package

3.4.8. Advice from Central and Local Government

Advice from, or sponsored by, Government and Local Government. Again, this is only a sample:

Thinkuknow : <http://www.thinkuknow.co.uk/parents/> run by CEOP, has sections for parents and children

Directgov:

http://www.direct.gov.uk/en/HomeAndCommunity/TechnologyInYourHome/InternetTechnologies/DG_10038607

GetSafeOnline: <http://www.getsafeonline.org/>

IdentityTheft.org: <http://www.identitytheft.org.uk/> (Home Office) – sections for consumers and business

Trading Standards: there appears to be no nationwide advice, though many individual locally-based offices do: eg

http://www.newport.gov.uk/_dc/index.cfm?fuseaction=tradingstandards.consumeradvice&contentid=cont104375;

http://www.birmingham.gov.uk/GenerateContent?CONTENT_ITEM_ID=6286&CONTENT_ITEM_TYPE=0&MENU_ID=1522;

<http://www.solihull.gov.uk/tradingstandards/internetshopping.htm>;

http://www.devon.gov.uk/web_internet_leaflet_devon.pdf

3.4.9. Instant Response Services

These are distinguished from the bulk of the Awareness and Educational programs in that they offer a means for some-one to get immediate advice if they are in distress. A few of these offer online contacts, mostly it is a phone-based service. Many of these have a wider agenda than simply the “Internet”

CEOP Report Abuse:

<http://www.ceop.gov.uk/reportabuse/index.asp>. Also contains links to NSPCC.

NSPCC: There4me:

http://www.there4me.com/siteaccess/S_Splash.asp. This service is not particularly well publicised, possibly because of lack of resources

Childline: <http://www.childline.org.uk/Pages/default.aspx> This is a telephone-based service in which NSPCC plays a part and which covers a wide range of situations in which children might feel distressed, of which Internet problems are only a small part.

StopItNow: <http://www.stopitnow.org.uk/>

Cyber-bullying / Kidscape – provides link to CEOP

BullyingUK:

http://www.bullying.co.uk/young_people/cyberbullying/index.aspx - offers email contact

Horse’s mouth – <http://www.horsesmouth.co.uk/> a online mentoring service

There does not appear to be any literature on the efficacy of these, and their associated problems. The following has been picked up by talking informally: These services are very resource-intensive. One of the main problems is that “clients” in distress may ring up an organisation which, though it offers assistance, can’t provide the precise help that is actually needed. This means that whoever picks up the phone / responds to a red button has to carry out a filtering exercise and decide whether to refer the client to some-one else (and

there are plainly problems just around that). A further problem area is calls from hoaxers or attention-seekers. All these services have to have a 24/7 element, which adds to the provider's cost. Once a "relevant" distressed client is identified, the extent of immediate and then longer-term support can be considerable. NAO should ask CEOP about their Report Abuse facilities and also to ChildLine, resources required, their experiences, and the associated costs.

3.5. International Research Initiatives

EU Safer Internet Program⁸⁴ This started as the Safer Internet Action Plan in 1999 and has been through a number of revisions and refundings since then. The current program is now funded through to 2013. The Program provides part of the funding for the IWF and also for CEOP. It also provides support for INHOPE, which is the international federation of hotlines similar to IWF.

Over the years it has produced detailed studies on hotlines⁸⁵, Internet Filtering programs⁸⁶, the efficacy of awareness and education programs⁸⁷, social networking sites⁸⁸ mobile phones⁸⁹, self-regulation⁹⁰, and cyber-bullying.

⁸⁴ http://ec.europa.eu/information_society/activities/sip/programme/index_en.htm

⁸⁵ http://ec.europa.eu/information_society/activities/sip/programme/workprogramme/wp2004_hotlines/index_en.htm

http://ec.europa.eu/information_society/activities/sip/projects/targeted/filtering/sip_bench/index_en.htm#results2008

⁸⁷ http://www.itu.int/newsroom/press_releases/2009/01.html;

http://ec.europa.eu/information_society/activities/sip/programme/workprogramme/wp2004_awareness/index_en.htm

⁸⁸ http://ec.europa.eu/information_society/activities/social_networking/docs/sn_principles.pdf

⁸⁹ http://www.gsmworld.com/gsm europe/documents/gsm_implementation_report.pdf;

http://ec.europa.eu/information_society/activities/sip/docs/mobile_2005/europeanframework.pdf

⁹⁰ http://ec.europa.eu/information_society/activities/sip/programme/workprogramme/wp2004_selfregulation/index_en.htm

4 Conclusions

It is possible to look at the statute book, find no criminal offences which directly relate to the Internet and conclude that there is no such thing as “Internet Crime”. It is possible to look at statistics for convictions and for the incidence of crime and make the same conclusion.

But by 2009 some 70% of the UK population have laptops or PCs at home and of those 93% now use broadband. This means that 65% of adults have broadband at home. The growth is now taking place among the less well-educated and technologically sophisticated, those who perhaps would prefer a personal computer to be more like most other domestic appliances such as tvs, music players and radio - where the controls are minimal and easy to use and there are no security issues. Personal computers are, by their nature open programmable devices even if the owners don't themselves want those facilities. Openness and programmability is what gives the personal computer its incredible flexibility and adaptability. Broadband connections bring much greater speeds and hence much more data per second and the user is now freed from the need to economise in Internet sessions. More material downloaded means more opportunity for malware to become implanted on the computers of victims. Under broadband there is no cost to the user in keeping the connection to the Internet continuously open – and while this occurs, an unprotected computer is highly vulnerable to attack.

The Internet also derives its flexibility and ability to provide the platform for new services because it too is based on open protocols. There are yet another multipliers: more time online, more data downloaded, cheaper personal computers with cheaper data storage has prompted experimenters and entrepreneurs to launch new data-intensive services such as social networking, media downloads, more extensive e-commerce sites, more complex and sophisticated e-banking and other financial services sites. It has also prompted Government to use the Internet as a way of delivering Government services, including the collection of tax revenue and the provision of a very wide range of information services.

Many of these new services also provide a vector for criminal behaviour. Indeed although some forms of Internet crime *modus operandi* are almost invisible, others rely on masquerading as genuine Internet facilities – fake websites, misleading emails, misleading social networking connections, downloads that contain logic bombs.

Not the least of the problems is that while most people develop an instinct for personal security in terms of familiar things such as the home, walking about in the street, carrying money and high value objects, and when making purchases in shops and markets, many of the Internet environments are new. The self-protective instincts are not there, the advice may not be there, and some of the remedies require significant technological sophistication.

In the circumstances it is not surprising therefore that for significant sections of the public there is a solid perception that “the Internet” is a source of crime and that speaking of “Internet Crime” is wholly justified.

But the Internet itself is a complex beast: at one level a series of physical connections enabling data to be sent via a succession of switches, at another a set of technical agreements and protocols, at yet another a set of complex commercial infrastructures, and yet still further subject to various types of law and regulation. Much of the discussion about Internet security and Internet governance is bedevilled by the understandable failures of the discussion participants to appreciate how the Internet works⁹¹.

In response to concerns about Internet security and crime a vast number of websites, leaflets and initiatives have sprung up. Some have been prompted by central and local government, some by publicly funded agencies such as the police and training standards, others have come from charities and NGOs, yet others from trade associations such as those that represent the banks. Most Internet Service Providers also offer their customers a combination of free general advice and the opportunity to buy in additional security services. Inevitably each piece of advice is coloured by the nature of its sponsorship. It is almost certainly true that anyone who takes the trouble to search out a wide range of these advice sources will end up with a pretty comprehensive set of measures to follow. But what is also almost certainly true is that few of these individual initiatives have been properly tested – are they easy for the target audiences to locate, are they properly and fully answering the questions the target audience may have? And, for government, are there gaps in the coverage – sections of the population which need advice and whose needs are not being adequately covered?

For government there are further issues: there are many overlaps and duplication in the coverage; some of the websites and leaflets appear not to have been touched since they were first published several years ago. Little research appears to have gone into designing them in the first place and little effort made to see if they were effective.

⁹¹ See for example the range of submissions made to the House of Lords *Personal Internet Security* report; <http://www.parliament.the-stationery-office.com/pa/ld200607/ldselect/ldsctech/165/16502.htm>

In a value for money exercise government has to ask itself if there are problems that need to be addressed, if these problems are not already being adequately covered by commercial and non-governmental bodies, and if there are still gaps, what precise response is an appropriate candidate for government action and expenditure.

In the Internet Crime domain there are few reliable direct statistics and without the notion of the size of the problem it is impossible to assess value for money.

Trends

The following trends seem worth commentary:

1. **Internet-based frauds and scams** of all kinds are probably the major threat to adult users of the Internet. The problem is the variety of forms and methods that these can take: -e-commerce sites that mislead and don't deliver, misleading emails, phishing attempts, various forms of identity theft. Some of the methods are principally forms of social engineering, others rely on exploiting technical weaknesses in personal computers and how they are used on the Internet. There is every reason to suppose that all the existing methods used by criminals will continue to be deployed but also that new methods will continue to appear. This suggests, at the least, the need for reliable continuously updated protective information to be made available to potential victims.
2. **Viruses and malware** are for the most part controllable by potential victims by the deployment of anti-virus software which is frequently updated.
3. **Spam** continues to plague the Internet emailing system. From the perspective of the end-user, the only protection is via spam-filters, probably those deployed by ISPs as opposed to those deployed on the user's own computer.
4. **Distressing and illegal images**, so far as one can tell, seldom present themselves to those who are not already looking for them, though it is reasonable to say that such seekers may find material more extreme and more distressing than they had planned.
5. **Cyber-harassment** between adults is likely to continue to grow but is in essence little different from bullying-in-person.
6. **Social Networking** in the sense of specific communities mediated by the environment of websites scarcely existed three years, though some of the oldest institutions on the Internet – the newsgroups and controlled email

lists – have always had a strong social element, as have Bulletin Board Systems (which predate the consumer-based Internet by some 15 years and Internet versions of which still thrive). What is interesting is the speed with which a particular social network can very quickly achieve large numbers of members – consider the “Twitter” variant just at the moment. And there is a corollary that almost certainly older networks fall out of favour – they can still claim a large membership as “resigning” is both complex and from the member’s perspective often unnecessary as there are no fees involved. Although there are generic security and safety issues with social networks, each one has its own particular problems in terms of information it allows/encourages members to publish about themselves.

7. **Small businesses** are likely to face frauds as well as malware. The problem for SMEs is that their internal systems are more complex than those used in the home, which means that more sophisticated technical measures may be required to promote security. At the same time though, they may not be of a size where they can afford on their own staff a specialist security technician/advisor. A further problem for small businesses is likely to be datatheft, in its most common *modus operandi* of copying important information to an external hard drive of USB stick and then walking out with it. The remedies for this are only partly in the technical domain.
8. **Threats to Children – Sexual** have had a great deal of publicity and for entirely understandable reasons. But there are grounds for worrying that some of the publicity may cause unnecessary concern. Most child abuse is carried out not by a stranger but some-one known to the family. Statistics which more properly relate to bullying between children – obviously a concern in itself – may be getting conflated with the likelihood that an adult is attempting to groom. The notion that children who meet people on the Internet and then go off with them may already be suffering from personal problems remains relatively under-explored.
9. **Threats to Children – Commercial** In contrast to the position in the United States where there is specific legislation to protect children, the Children’s Online Privacy Protection Act, 1998 (“COPPA”) and where there is a significant amount of literature, this topic has so far not received much attention in the United Kingdom.
10. **Older People** One sector vulnerable to “Internet Crime” that does appear to being neglected are the over 65s. Ofcom reports that personal computer ownership and Internet usage is still low among the over 75s but it seems a reasonable projection to suggest that the over 65s, and those who are about to reach that age are likely to become the next wave of customers, many other sectors already becoming almost “complete” But older people are already vulnerable to a variety of scams, criminals being attracted both by

the possibility that their victims may be easily confused and that they have wealth that is worth stealing. The Internet offers many attractions to the over 65s – increased social contacts, a response to loss of mobility, information specific to their needs (some of it provided by Government which sees Internet provision as a means of cutting the costs of delivering services). But the rate of change and the “open” nature of personal computers and the Internet itself referred to above also make it much easier for an older person to be purposefully confused by criminals.

Possible Recommendations

The following are some recommendations for further action:

1. The collection of reliable data is a pre-requisite for policy formation. Starting a new dataset is likely to be expensive and routes need to be found to take advantage of circumstances in which relevant data is already being collected. Specifically:
 - Police Crime Incident Report facilities, which are filled in when a potential crime is first reported and is then used as an investigation progresses, do not (with a few exceptions) record any “computer” or “Internet” dimension in such a way that statistical data can easily be subsequently extracted
 - It would be interesting to know if similar facilities and as a result a similar enhancement could be deployed at the offices of Trading Standards
 - The Crown Prosecution Service records convictions but does not presently record if the *modus operandi* has a computer dimension
 - APACS currently rolls into its statistics of “customer not present” frauds, telephone, mail order and online activities. It would be helpful if they could in future split these down as they did in their 2007 Report, though not the latest
 - CIFAS similarly might be encouraged to get its members to report more specifically on the cyber- and Internet forms of fraud
 - ChildLine, the main “instant response” service for children, deals with all forms of bullying and abuse. Although its main focus is rightly to help the child it would be useful if whatever system is used to record contacts between the service and its

clients contains fields which can be subsequently used for statistical analysis. How far are the problems Internet-related, mobile-phone related, take place “in person”? How far are the problems child-on-child, known adult on child, or “stranger danger”?

- The House of Lords *Personal Internet Security* Report contained a recommendation for a security breach report law. There are a number of advantages in terms of information security governance in such a law but another benefit is that it will produce a good source of statistics.
 - BCS is limited by the fact that there are many calls on its resource to explore areas of crime and that it is felt that no interview can last longer than 45 minutes without alienating interviewees.
 - National Fraud Reporting Centre was announced by the Attorney General in April 2008 and had what appears to have been a launch in March 2009. However at the time of writing it is still not up and running. It is supposed to “work with” the City of London Police and the new Police Central E-Crime Unit. From its name, at the very least, it will be tasked with receiving reports. There is an opportunity here for it to categorise frauds by *modus operandi* including the various Internet-based frauds discussed in this review. In that connection it is worth comparing with the US Internet Crime Compliant Center (IC3) - <http://www.ic3.gov/about/default.aspx> - which is a partnership between the FBI and that National White Collar Crime Center⁹².
2. If statistics are to be gathered there needs to be some generally-agreed set of definitions and a forum in which the agreements can be made. Government seems to be the most obvious sponsor of such an initiative. Since most of the statistics will be for incidents which have not been tested in court, some guidance will have to be given about standards of report reliability.
 3. The advantage to government of having more reliable statistics will extend beyond determining value for money in advice services. Although these are matters beyond the remit of the current NAO report, government also needs to take a view on future provisions for general

⁹² <http://www.nw3c.org/>

police training in computer and Internet matters, for the numbers of specialist police officers and civilian forensic staff, and for training within the CPS and judiciary.

4. The Government already has in place a policy to rationalise its various websites, closing many down and concentrating the balance under the “DirectGov” banner. Once some better statistical data is in place it should be possible to decide whether the combination of existing websites from NGOs and commercial interests fully meets the needs of the public as a whole. In so far as they don’t and in so far as a central government-sponsored advice service is required the statistics should also point to the scope extent and resource-requirements of such a service. It may well be that such an advice service can also provide the forum for defining and collecting the statistical data. The savings from the existing duplicated and fragmented services could be directed towards a possible one-stop shop.
5. A further area to research are the so-called Instant Response services, where, via a website, email or telephone call, advice and perhaps more is available. Anecdotes, as opposed to proper research, seems to point to the following: Many of the people who ring a specific service such as CEOP or ChildLine have problems which are outside the specific remit and resource of those services. Yet the person responding has to spend time assessing and filtering the query. Often they are dealing with people in distress, so that a simple “Sorry, not us” response is inadequate. In other instances the actual problems of the “client” may be quite complex and long-term. Is the answer “Go to this site and you’ll find instructions”, or “You need psychiatric help”, or “You need to be taken to a place of safety”, or “You’ll have to collect evidence before we can act”, or “You need to install some specialist software, this is how you do it”? The Research would need to cover: the extent to which Instant Response seems to be called for, as opposed to a more passive means of providing information, and resource implications.
6. Throughout this review it will have been seen that a great deal of information and Internet safety is available to the public from charities, NGOs, trade associations, computer companies and individual companies that interact with the public via the Internet. The question that arises therefore is how “complete” this coverage is in terms of the totality of advice and support one believes the various sections of the public ought to be receiving. Almost certainly there will turn out to be gaps which will need to be fulfilled by government. The question to be asked is: does government have a mechanism for knowing where these gaps exist?