



UK CYBERCRIME REPORT 2009

Stefan Fafinski
Neshan Minassian
Invenio Research
September 2009



Preface

This particular report, published in September 2009, is the third consecutive UK Cybercrime Report published by Garlik in an attempt to illuminate the so-called 'dark figure' of cybercrime,

As more UK households have Internet access, the greater the potential number of victims for cybercriminals to exploit. In 2009, 18.3 million households in the UK – that is 70% of all households – had Internet access. This is an increase of 11% (around 2 million households) since 2008 and 28% (around 4 million households) since 2006. More households are connected via broadband each year – of those households with Internet access, 90 per cent had a broadband connection in 2009, an increase from 69% in 2006.¹

Given the ever-increasing presence of the UK online in connection with the economic downturn, this report focuses on an *estimated* quantification of cybercrime for the calendar year 2008 whilst considering the effect that the economic climate may have had on the prevalence of different types of cybercrime. For the first time, the report also considers property and Land Registry fraud.

It is not easy to count any sort of crime. Cybercrime is no exception, and there are many pertinent reasons as to why cybercrime is particularly difficult to quantify. This is explored in more detail in Appendix A of the report.

¹ National Statistics (26 August 2009) <<http://www.statistics.gov.uk/CCI/nugget.asp?ID=8>>



Executive summary

UK cybercrime has rebounded to worrying levels, not seen since 2006, as a result of the recession and consumer complacency, according to Garlik's annual UK Cybercrime report, now in its third year.

The report, which analyses publicly available data to build a comprehensive view of cybercrime in the UK, revealed that during 2008 cybercriminals adapted to the social and economic changes in the UK to exploit victims in new ways and commit over 3.6 million criminal acts online (that's over one every 10 seconds). In addition, the researchers believe that there is a growing complacency amongst consumers, demonstrating poor understanding of their responsibility to protect their personal information against fraud.

One of the most significant changes in cybercrime has been the 207% increase in account takeover² fraud indicating that criminals have now shifted their efforts from opening new accounts with stolen identities to accessing existing accounts. Savvy criminals have got round the drying up of available credit in the current economic climate to maintain their illegal activities.

The report also highlights that online banking fraud has increased by a staggering 132%, with losses totalling £52.5 million, compared to £22.6 million in the previous year. This sharp rise can be mostly attributed to nearly 44,000 phishing websites specifically targeting banks and building societies in the UK.

The total number of cybercrimes has increased annually between 2006 and 2008, however, the good news is that sexual offences have decreased as a category each year. All other categories dipped in 2007 but then in 2008 bounced back above their 2006 figure.

² Account takeover means the ability to access individuals' accounts, whether these be bank accounts, mail accounts, social networking accounts and so on, to commit fraud.



One possible explanation for the sharp rise in cybercrime lies in the consumer reaction to it. Identity theft in particular received a great deal of media and public attention in 2006. As a result, many consumers took the first steps to protect themselves, buying shredders and anti-malware software to feel secure but have since become too complacent and as a result have been hit by the next wave of cybercrime. As threats shift and change, it is essential for consumers to take steps for their own safety: even if they think that it is 'someone else's problem'. It is not. Consumers need to be smart online and stay one step ahead of the cybercriminals.

Category	2008	2007	2006	Change 07/08
Identity theft and identity fraud	86,900	84,700	92,000	+2.6%
Financial fraud	207,700	203,700 ³	207,000	+1.9%
Online harassment	2,374,000	2,240,000	1,944,000	+6.0%
Computer misuse (excluding viruses)	137,600	132,800	144,500	+3.6%
Sexual offences	609,700	617,500 ⁴	850,000	-1.3%
Total	3,415,900	3,278,700	3,237,500	4.2%

³ APACS reclassified 2007 figures in 2008. 2008 Cybercrime Report figures recalculated on that basis.

⁴ Please note that the 2007 figure recalculated on the basis of findings from Wolak, J et al. 'Online Victimization of Youth: Five Years Later' (National Center for Missing and Exploited Children, 2006) reducing percentage of victimisation from 20% to 13%.



Identity theft and identity fraud

Identity theft is the assumption of the identity of another person, living or dead, irrespective of the motivation underlying this course of action. For example, taking on the identity of a dead person and living life as them, having abandoned one's own identity. By contrast, identity fraud is the transient or partial assumption of another's identity.

According to CIFAS, the UK's fraud prevention service, the 2008 figures relating to fraud break down as follows:

Identity fraud ⁵	77,642
Application fraud ⁶	77,023
Impersonation ⁷	62,658
Total	217,323

This represents a decrease from 2007 of 0.9%.⁸ However this headline decrease is slightly deceptive, as although there appears to be an overall decrease (based on the figures above), the reality is that certain other areas of fraud have experienced a significant increase over the last 12 months.

⁵ Includes cases of false identity, identity theft and account takeover.

⁶ Applications containing at least one material falsehood.

⁷ Fraudulent operation of the victim's account or facility as the offender's own.

⁸ 2007 total figure 219,506. See CIFAS '2007 Fraud Trends' <www.cifas.org.uk/default.asp?edit_id=790-57>.



Perhaps the most notable example of this is the 207% increase in facility takeover fraud (also known as account takeover), the scale of which has been described by CIFAS Head of Communications, Kate Beddington-Brown, as ‘truly alarming’.⁹ Moreover, there has been an increase of 66% in the misuse of facilities. The table below shows the increase in the frequency of these types of fraud between 2007 and 2008:¹⁰

	2007	2008	Change
Facility takeover fraud	6,272	19,275	+207%
Misuse of facility	23,400	39,447	+69%

As CIFAS comments, fraudsters know that lending criteria have become more stringent as a result of the credit crunch, and that application fraud is likely to be unsuccessful. They are, therefore, turning their attempts to other types of fraud.¹¹

As was the case during 2007, the prevalence of the victims of fraud remains highest in the South East of London with only three postal districts of the top 30 ‘fraud hotspots’¹² being found outside London.

Based on offender studies,¹³ it is estimated that around 40% of identity frauds are facilitated online. Given this, it is estimated that there were approximately **86,900 cases of online identity theft and identity fraud in 2008.**

⁹ CIFAS ‘2008 Fraud Trends’ <www.cifas.org.uk/default.asp?edit_id=896-57>.

¹⁰ Ibid.

¹¹ Ibid.

¹² Experian, ‘Victims of fraud dossier, Part IV’ (May 2008)

¹³ Finch, E. (2009) ‘Strategies of Adaptation and Diversification: the Impact of Chip and PIN Technology on the Activities of Fraudsters (forthcoming).



The profile of identity frauds has changed with a significant shift toward facility takeover within the total figure for identity fraud. With the declining availability of credit throughout 2008 and increased stringency of credit checking, fraudsters seem to have adapted and diversified into alternative strategies of identity fraud. This profile is likely to continue into 2009 in line with the continued restricted availability of credit. Consumers should therefore remain vigilant for malware¹⁴ which could lure them into giving out account information on bogus sites. Fraudulent sites are increasingly linked to current affairs rather than the 'traditional' fake banking sites. Consumers should not remain complacent and ensure that they continually update anti-virus and anti-spyware software and keep their operating systems updated. Measures that would have been adequate to protect consumers in 2007 should be updated to counter continually-evolving threats.

¹⁴ Malware - short for *malicious software*, is software designed to infiltrate a computer without the owner's knowledge or consent.



Financial fraud

Financial fraud and identity theft are closely related, since the misuse of a stolen identity can be used for financial gain. Of course, not every instance of identity theft relates to a financial fraud, since stolen identities can be used for many different purposes. Online financial fraud can also be achieved with false credit card information and some limited identity information, but not necessarily enough to assume the victim's identity fully.

In 2008, in relation to *all* crime:

- Losses from plastic card fraud rose by 14% from £535.2m in 2007 to £609.9m in 2008.
- Online banking fraud losses increased by 132% from £22.6m to £52.5m. This constitutes 8.6% of the total figure of loss for 2008.
- Cardholder-not-present (CNP) fraud loss has increased by 13% from £290.5m to £328.4m and accounts for a significant 54% of all card fraud losses
- The total value of online shopping in 2008 was £41.2 billion¹⁵

This increase is commented upon in the British Crime Survey:

The 2008/09 BCS shows there has been an increase in plastic card fraud, with 6.4 per cent of plastic card users being aware that their cards had been fraudulently used in the previous 12 months, compared with 4.7 per cent of card users in the six months to March 2008.¹⁵ This is also a rise from 3.7 per cent in 2005/06 when questions on plastic card fraud were first added

¹⁵ APACS, 'Fraud the Facts 2009' <http://www.apacs.org.uk/resources_publications/documents/FraudtheFacts2009.pdf>



to the BCS. It is also considerably higher than the risk of victimisation for other types of theft, for example, 1.5 per cent had been a victim of theft from the person in the 2008/09 BCS¹⁶

The highest proportion of loss in the UK was in the South East of England where £204.7m of the total £609.9m was lost, constituting 27% of overall losses on UK cards (both in the UK and abroad). It is interesting to note that the South West of the UK saw the highest percentage increase in plastic fraud losses (up by 64% from £11.8m to £19.8m), followed closely by Scotland (up by 61% from £11.5m in 2007 to £18.5m in 2008) and East Anglia (up by 58% from £4.8m to £7.6m).

£181.7m of card fraud took place on the Internet in 2008 - 55.3% of total CNP fraud losses. This figure is up 2% since 2007 when losses were £178.3m. Although e-commerce fraud accounts for a lower proportion of overall CNP fraud losses than it did in 2007 (61%), it merely indicates that fraudsters are moving towards other CNP channels, such as the telephone. Assuming an average loss of £875¹⁷ per fraud, there were approximately 207,700 cases of online financial fraud in 2008.

Counterfeit card losses have increased by 18% from £144.3m to £169.8m. The increase has slowed from the 46% rise in 2007¹⁸. It appeared that fraudsters are finding it harder to commit this type of fraud in the UK due to the increased usage of Chip and PIN. However, fraudsters still steal card details in the UK to make counterfeit cards for use abroad where such measures are yet to be introduced or are not used as extensively as they are in the UK.

¹⁶ Home Office Statistical Bulletin, Crime in England and Wales 2008/2009; Volume 1, Findings from the British Crime Survey and Police Recorded Crime, 85.

¹⁷ Garlik, UK Cybercrime Report 2007.

¹⁸ APACS, 'Fraud the Facts 2009'



Encouragingly, lost and stolen card fraud losses has seen a 4% decrease during 2008 compared to 2007 from £56.2m to £54.1m. It is safe to say that this is largely attributable to the continuing establishment of chip and PIN.

Losses from online banking fraud have increased by a significant 132%¹⁹ from the previous year with losses totalling £52.5million. (£22.6million in 2007). This sharp increase can be attributed, in part, to there being 43,991 phishing²⁰ websites targeting UK banks and building societies in 2008, up 171% from 25,797 in 2007. As with identity fraud in general, consumers need to increase their vigilance. Phishing sites are becoming more prevalent and increasingly sophisticated.

¹⁹ APACS, 'Fraud the Facts 2009'

²⁰ APACS, 'Fraud the Facts 2009'. Phishing is the criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic form.



Online harassment

This category of cybercrime involves online harassment: the use of a computer to cause a personal harm such as anxiety, distress or psychological harm, including abusive, threatening or hateful emails and messages and the posting of derogatory information online.

There are no comprehensive public statistics kept on victims of online harassment or cyberstalking by ISP's, government or police (British Crime Survey).

However, given the number of Internet users and their online communities is increasing and the number of incidents of police recorded (all) harassment is roughly constant, it can be presumed that, as Internet use increases, the number of instances of online harassment also increases. The Internet makes harassment and threatening behaviour easier; there is no need for physical confrontation. Moreover, repeated threatening or alarming messages may be sent relatively easily. More sophisticated cyberstalkers use programmes to send messages at regular or random intervals without being physically present at their computer.

There is no simple definition of the terms 'online harassment' or 'cyberstalking'. Indeed, the terms are often used interchangeably. One of the simplest definitions of cyberstalking is 'the use of electronic communication including, pagers, mobile phones, emails and the Internet to, bully, threaten, harass, and intimidate a victim'.²¹ Online harassment can be seen as an element of cyberstalking, which has the additional factor of pursuit via electronic means:

The distinction between harassment and cyberstalking is that cyberstalking is characterized by pursuit and fear²²

²¹ Maxwell, A, 'Cyberstalking' (Auckland University Department of Psychology, June 2001) available at <www.netsafe.org.nz/ie/downloads/cyberstalking.pdf>.

²² Harvey, D, 'Cyberstalking and Internet Harassment: What the Law can Do' (Netsafe II: Society, Safety and the Internet Conference Proceedings, 2003) available at <www.netsafe.org.nz/downloads/conference/netsafepapers_davidharvey_cyberstalking.pdf>; Ellison, L and Akdeniz, Y, 'Cyber-stalking: the Regulation of Harassment on the Internet' (1998) Criminal Law Review Special Edition: Crime, Criminal Justice and the Internet 29.



Online harassment can be further divided into direct and indirect harassment. Direct harassment includes: threats, bullying, or intimidating messages sent directly to the victim via email or other Internet communications mediums, and/or the use of technological means to interfere with a victim's use of the Internet such as hacking or denial of services attacks. Indirect harassment includes – but is not limited to: spreading rumours about the victim in Internet discussion forums; subscribing the victim to unwanted online services, or sending messages to others in the victim's name²³.

In 2008, 16 million households in Great Britain (65%) had Internet access. This is an increase of just over 1 million households (7%) over the last year and 5 million households (46%) since 2002. Estimates for Great Britain are provided to give a time series, as UK estimates are not available prior to 2006.²⁴

Almost 16.5 million (65%) UK households including Northern Ireland had access to the Internet. This was an increase of 1.2 million households (8%) since 2007.²⁵

Facebook alone currently has 300 million active users, 150 million of which logon at least once a day. Each user has on average 130 'friends', with the fastest growing demographic being in those who are 35 years old and over.²⁶ Other social networking sites such as Bebo, Myspace and Twitter are also seeing an increase in their number of users.

The most recent official statistic concerning victimisation estimates that 8%²⁷ of adults using the Internet are victims of online (e-mail) harassment.²⁸ Therefore, given an adult population on the Internet of 29.7 million,²⁹ it is estimated that there were **approximately 2,374,000 instances of online harassment in 2008.**

²³ Ibid.

²⁴ Internet Access in the UK 2008 available at <http://www.statistics.gov.uk/CCI/nugget.asp?ID=8>

²⁵ Ibid.

²⁶ <http://www.facebook.com/press/info.php?statistics>

²⁷ British Crime Survey additional report: Mobile phone theft, plastic card and identity fraud: Findings from the 2005/06 British Crime Survey (Supplementary Volume 2 to Crime in England and Wales 2005/06) (15 May 2007)

²⁸ Receipt of an e-mail which was considered by the recipient to amount to a course of harassment or to be personally offensive

²⁹ 2007 figure of 28 million increased by 6%. Office for National Statistics, 'Internet Access 2008' <http://www.statistics.gov.uk/pdfdir/iahi0808.pdf>



The recent conviction of Keely Houghton, 18, for posting death threats on Facebook in a landmark case highlights the growing recognition of online harassment as a serious issue. Yasmin Joomraty, a lawyer at Laurence Kaye Solicitors, a firm of digital media specialists, said: "Harassment, even online, comes under the Protection from Harassment Act and can create both a civil and a criminal outcome. Though this case does not seem to me to mark a turning point necessarily, people do have to watch what they say online."³⁰

The sheer number of users of these network sites makes them intrinsically difficult to police, notwithstanding the fact that increasing numbers of convictions are being secured for various forms of harassment online.

³⁰ See <http://www.timesonline.co.uk/tol/news/uk/crime/article6805567.ece>



Computer misuse

This category of cybercrime is reserved for conduct that falls within the Computer Misuse Act 1990 (as amended by the Police and Justice Act 2006). It encompasses both basic and aggravated hacking (where a system is accessed without authorisation with the intent to commit further offences) and any unauthorised acts with intent to impair, or with recklessness as to impairing the operation of a computer.

There were 2.16 million business enterprises registered for VAT and/or PAYE in March 2008, compared to 2.10 million in March 2007, a 3.0 per cent increase.³¹ Of these corporate businesses (companies and public corporations) represent 56.6 per cent of total enterprises; Sole proprietors represent 25.4 per cent of total enterprises; Partnerships represent 14.1 per cent of total enterprises; General government and non-profit making bodies represent 3.9 per cent of total enterprises.³²

Just under 50% of UK businesses experienced a security incident (around 860,000). The number having a serious breach has stayed constant at around 25% (around 430,000).³³

³¹ Previous reports used data provided for VAT registration alone (1.67m in 2007); official statistics now use a broader definition of 'business'. Applying a 3% rise to 2007 figures gives a total of 1.72m.

³² Registered businesses increase by 3%; see <http://www.statistics.gov.uk/cci/nugget.asp?id=1238>

³³ Information Security Breaches Survey Technical Report conducted by PWC and found out [www.pwc.co.uk/pdf/BERR_ISBS_2008\(sml\).pdf](http://www.pwc.co.uk/pdf/BERR_ISBS_2008(sml).pdf); 25% of 1.72m comparing like-for-like with 2007.



16% of businesses experienced an attack from an unauthorised outsider (including hacking attempts) (**137,600 incidents**).

Computer misuse is categorised under the same 'Other frauds' heading for police recorded crime as the much more commonly recorded offence of making off without payment.³⁴ 127,949 reported crimes fell into this category in 2006/07, 118,407 in 2007/2008 and 122,569 in 2008/09.³⁵ Over the same period, approximately 296,769 burglaries from non-dwellings were recorded. This represents a fall by 2% from the number recorded in 2007/08 (approx 303,000)³⁶.

Over the same period, approximately 296,769 burglaries from non-dwellings were recorded. This represents a fall by 2% from the number recorded in 2007/08 (approx 303,000)³⁷.

³⁴ Theft Act 1978, s.3.

³⁵ Home Office Statistical Bulletin, Crime in England and Wales 2008/2009; Volume 1, Findings from the British Crime Survey and police recorded crime; page 139.

³⁶ Ibid.

³⁷ Ibid.

Sexual offences

This category of cybercrime covers a range of conduct that has an objectively ascertainable sexual element. It includes paedophilic activity such as grooming a child for sexual activity.

There was a 3.9% decrease in the number of sexual offences recorded in 2008³⁸ in comparison to 2007³⁹. The vast majority of these cannot be committed online since they require physical sexual contact between perpetrator and victim.

The most relevant sexual offence in terms of online behaviour is that of 'meeting a child following sexual grooming'⁴⁰, which is defined as intentionally meeting⁴¹ a person under 16⁴², having met or communicated on at least two earlier occasions with the intention to commit a 'relevant offence'⁴³.

Research by Ofcom has found that social networking sites in particular are extremely popular among children in the UK. 49% of children aged eight to 13 have an online profile compared to just 22 per cent of over 16-year-olds. While just over half of these children use the sites to make new friends, 43% say their parents set no rules for their use of networking sites.⁴⁴

³⁸ Number of sexual offences recorded in 2008 was 51,488; Home Office Statistical Bulletin, Crime in England and Wales 2008/2009; Volume 1, Findings from the British Crime Survey and police recorded crime; page 138

³⁹ Number of sexual offences recorded in 2007 was 53,477; Home Office Statistical Bulletin, Crime in England and Wales 2008/2009; Volume 1, Findings from the British Crime Survey and police recorded crime; page 138

⁴⁰ Sexual Offences Act 2003, s.15

⁴¹ Or travelling with the intention to meet.

⁴² Without reasonable belief that the person was 16 or over.

⁴³ Broadly speaking, a range of child sex offences.

⁴⁴ See <http://news.bbc.co.uk/1/hi/technology/7325019.stm>



The extent of children being targeted online for sexual purposes is difficult to evaluate. However, there have been some surveys of children's experience online. In the US, the first Youth Internet Safety Survey was conducted in 1999 and 2000 and revisited more recently in 2005, reported in 2006.⁴⁵ In 2005, decreased proportions of youth Internet users were receiving unwanted sexual solicitations – from 19% to 13%, or approximately one in seven. This was, however, an American study, although given the tendency for the UK to lag the US slightly, it is reasonable to assume that, in 2008, the level of such victimisation in the UK would be similar to that in the US in 2005/06.

Approximately 80% of adults with children between five and 15 stated that at least one child in the household had accessed the Internet at some time.⁴⁶ 95% of young adults between 16 and 24 access the Internet.⁴⁷ It is therefore reasonable to assume, as a conservative estimate, that 60% of children between five and 15 access the Internet.

Assuming, then, that 60% of children between five and 15 access the internet, then given a population of approximately 7,817,000 between five and 15⁴⁸, it follows that around 4.69 million access the Internet and there were therefore **an estimated 609,700 instances of unwanted sexual approaches** in 2008. However, there are no comprehensive recent statistics on the extent of the problem in the UK. This is disconcerting as there is consequently no official reflection as to the extent of this problem. For 2007/08 the police recorded figure of sexual grooming offences was 272.⁴⁹ For 2008/09 the recorded figure was 315,⁵⁰ a 16% increase.

⁴⁵ Wolak, J et al., 'Online Victimization of Youth: Five Years Later' (National Center for Missing and Exploited Children, 2006) <http://www.missingkids.com/en_US/publications/NC167.pdf>

⁴⁶ British Crime Survey additional report: Mobile phone theft, plastic card and identity fraud: Findings from the 2005/06 British Crime Survey (Supplementary Volume 2 to Crime in England and Wales 2005/06) (15 May 2007)

⁴⁷ British Crime Survey additional report: Mobile phone theft, plastic card and identity fraud: Findings from the 2005/06 British Crime Survey (Supplementary Volume 2 to Crime in England and Wales 2005/06) (15 May 2007)

⁴⁸ UK population 2008 (aged 5-15) 7,817,000 National Statistics at <www.statistics.gov.uk/populationestimates/svg_pyramid/ew/index.html>

⁴⁹ Home Office Statistical Bulletin, Crime in England and Wales 2008/2009; Volume 1, Findings from the British Crime Survey and police recorded crime; page 138

⁵⁰ Ibid.



Land Registry fraud

There have been concerns this year that the Land Register is 'too open to fraud'. Organised criminals have increasingly used the Land Registry to transfer ownership of a house fraudulently, to sell it, or to apply for large mortgages secured on the property. In March 2009, a BBC investigation applied to change details of house ownership without being asked for proof of identity.⁵¹ Changing the service address for a property will mean that any correspondence from the Land Registry is sent to the new address. As Detective Inspector Colin Richards of Merseyside Police commented, once the service address is changed, criminals can pose as a builder owed money for work on the property and instigate a civil action to recover the 'debt'. In the absence of a reply to the court from the 'defendant', the court may order the house to be sold with the money going to the criminals posing as the claimant. The criminals may also pose as the property owner, agree to the sale, and receive the net proceeds: thereby gaining the entire sale value of the property.⁵² Simon and Christine Rowntree had a £325,000 mortgage secured on their property without their knowledge. There are over a dozen cases currently under investigation.

However, in 2007, the Land Registry stated that 'no one can own a property that is registered to someone else' and that 'there is no evidence that fraud has resulted from the availability of information from Land Registry'.⁵³

⁵¹ BBC News, 'Land register "too open to fraud"' (30 March 2009).

⁵² BBC News, 'How a fraudster "stole our house"' (31 March 2009).

⁵³ The Register, 'Land Registry denies ID fraud risk' (15 August 2007).



On 15 May 2009, Eleanor Laing MP, asked what mechanisms to prevent fraud are used by HM Land Registry. Michael Wills MP, from the Ministry of Justice, responded that:

...measures already implemented include:

- publication of Land Registry Public Guide 17 – How to safeguard against property fraud and Public Guide 02 – Keeping your address for service up to date, which advise property owners to record current contact addresses with Land Registry...
- enhanced ID requirements...;
- anti-fraud training for all Land Registry caseworkers; and
- the introduction of IT systems to assist in identifying suspect cases.⁵⁴

On 20 May 2009, Mrs Laing asked the Secretary of State for Justice to quantify:

- (1) how many convictions there have been for offences of property title theft in respect of (a) mortgaged, (b) non-mortgaged and (c) vacant properties in each of the last 10 years;
- (2) how many convictions there have been for offences of fraud in relation to property leases in each of the last 10 years;
- (3) how many convictions for offences of property transfer fraud there have been in each of the last 10 years;
- (4) how many convictions for offences of mortgage fraud there have been in each of the last 10 years;
- (5) how many convictions for offences related to property fraud there were in each of the last 10 years.

⁵⁴ Hansard HC Deb (2008-09) VWA 1102 W *(15 May 2009).

The answer, from Maria Eagle MP, illustrated the problem in quantifying official statistics for this type of fraud. The statistics given were for the offence of 'obtaining property by deception' which was repealed in January 2007 and subsumed into the broader set of fraud offences; however, 'property' in this context includes money and all other property, real or personal, including things in action and other intangible property.⁵⁵ It does not specifically break out offences against 'property' in the everyday sense of the word (that is, 'domestic dwelling'):

The statistics provided were for fraud offences where either the statute or the offence description identifies the fraud as solely relating to either 'property fraud' or 'mortgage fraud'. A number of other fraud offences may include 'property or mortgage fraud', but as the individual circumstances of the offence are not held on the court proceedings database maintained by the Office for Criminal Justice Reform, it is not possible to separately identify them...

Court proceedings data for 2008 will be available in the autumn of 2009.⁵⁶

Moreover, on 10 June 2009, Caroline Spelman MP asked the Secretary of State for Justice what estimate he has made of the number of instances of property fraud involving fraudulent applications to the Land Registry for changes of address in the last 12 months. Michael Wills MP replied:

It has taken longer than expected to collate the information requested. I will write to the Hon. Member as soon as this is available.⁵⁷

There are, therefore, no official statistics on the extent of Land Registry fraud, although the BBC reports that £35million has been paid in compensation since 2005.⁵⁸

⁵⁵ Theft Act 1968, s4(1).

⁵⁶ Hansard HC Deb (2008-09) WA 1446W (20 May 2009).

⁵⁷ Hansard HC Deb (2008-09) WA 889W (10 June 2009).

⁵⁸ BBC News, 'Land register "too open to fraud"' (30 March 2009).



Summary

As in each of the past two years, there has been an overall increase in the estimated number of cybercrimes within the UK, with all categories of conduct, bar sexual offences, increasing in prevalence. However, with the exception of online harassment, figures fell from 2006 to 2007 and then rose again from 2007 to 2008.

One possible explanation for this lies in the consumer reaction to cybercrime. Identity theft in particular received a great deal of media and public attention in 2006. As a result of this, many consumers took steps to protect themselves both online and offline, which they assumed would be sufficient but they actually needed to do more. Sales of domestic shredders and anti-malware software rose in response to the media panic portrayed in relation to cybercrime at the time. This increased awareness coupled with taking relatively simple and practical steps to deter certainly the more casual cybercriminal may have contributed significantly to the drop in the majority of categories of cybercrime between 2006 and 2007. The only category that increased during this period was online harassment; driven by the marked rise in the use of social networking sites and thus the greater arena of potential victims.

However, figures for identity-related frauds and financial frauds in particular have risen again from 2007 to 2008 to (roughly) 2006 levels. While consumers took sensible steps to protect themselves against 2006 threats, cybercriminals have adapted and diversified their approaches such that new vulnerabilities are being exploited. If consumers have not taken steps to keep their protection up to date, then it follows that they will be more at risk. Anti-spyware and anti-malware software is only effective against the threats identified as being in existence at the time it is released. While there will always be a 'threat gap' between malware in the field and that against which software protection is offered, the longer the protection remains static, the greater the potential for a threat to be realised.

Consumer complacency may therefore be at the root of the increases in cybercrime from 2007 to 2008. While education and raising awareness of the issues may help to bridge this gap, it can also be argued that education and awareness campaigns cannot help individuals who do not think that it is their personal responsibility to protect themselves from cybercrime. This then raises the issue of who should carry the responsibility of protecting individual and commercial concerns from cybercrime. A survey commissioned by Get



Safe Online⁵⁹ found that 15% of people think that it is their own responsibility to protect themselves, 49% think it should be the responsibility of 'big business' and 11% think that it should be a government responsibility. However, consumers must recognise that without taking steps to protect themselves then they will be exposed to a greater level of risk than they might otherwise have appreciated. A recent survey commissioned by VeriSign⁶⁰ has highlighted the need for education on how online consumers might better protect themselves, showing that, despite the fact that many consumers claim to be security conscious and are cautious when buying goods online, there are still 18% of Londoners who do not bother to check a website's security settings before entering into an online transaction.

Consumers should not, therefore, turn a blind or ignorant eye to the risks of cybercrime. It remains as real a risk as it did in 2006 when there was a greater level of coverage on the issue. Since then, other matters of public concern have come to the fore, particularly those associated with the recession. However, cybercrime remains a concern which should not be ignored. Indeed, as considered in last year's report, there were fears that the recession would cause a rise in crime. The Home Office forecast⁶¹ that acquisitive crime would rise in 2008. This report also forecast that individuals with access to technology and the skill to use it might well have lifestyles to protect which have been funded by access to credit in the past. If credit is denied in their own identity, then a more creditworthy identity may be adopted to meet increasingly stringent vetting requirements. This prediction has been reflected in the rise in facility takeover fraud which increased by 207% in the past year as cybercriminals recognised that lending criteria would become more stringent and therefore moved from application fraud to other means of achieving their aim.

As the UK comes out of recession and access to credit becomes easier, it is foreseeable that there will be a return to application fraud which requires less effort on the part of the fraudster than facility takeover. However, the increase in successful phishing attacks in the past year may result in fraudsters continuing or expanding this potentially lucrative means of operation. Consumer vigilance remains key: as threats shift and change, it is essential for consumers to realise that they must take steps for their own safety and will be at increased risk without doing so: even if they think that it is 'someone else's problem'. It is not.

⁵⁹ National Campaign Launched to Get UK Safe Online' <http://www.getsafeonline.org/nqcontent.cfm?a_id=1432#_edn1> (October 2005).

⁶⁰ Verisign, <[http://www.imrg.org/8025741F0065E9B8/\(httpPressReleases\)/OCD9C082DE9B46B480257633003D2E08?OpenDocument](http://www.imrg.org/8025741F0065E9B8/(httpPressReleases)/OCD9C082DE9B46B480257633003D2E08?OpenDocument)> (September 2009)

⁶¹ Kennedy, S, 'Recession will bring big rise in crime and race hatred, says Home Office' *The Times* (1 September 2008)



Appendix A - Counting cybercrime

It is not easy to count any sort of crime. Cybercrime is no exception, and there are many pertinent reasons as to why cybercrime is particularly difficult to quantify. First, the criminal conduct may not be noticed. For instance, if an online banking fraud comprises multiple low-value transactions across a bulk body of victims, the victims may not spot the minor discrepancy in their accounts. Alternatively, the victim might not know that the observed conduct is criminal. For instance, in relation to virus attacks, there is a general public and industry perception that no-one has broken the law.⁶² The victim may also choose not to report the crime to the authorities. This may be because of a feeling that nothing can be done because it is too late to rectify the harm caused, or that there is little chance that the police will identify, detain and prosecute the offender. Alternatively the perpetrator may be difficult or impossible to identify since the Internet offers relative anonymity and an easy way to shield identity. The police have limited resources and expertise to tackle cybercrime so may discourage the victim from pursuing a formal complaint for a minor occurrence as investigation would be too difficult. Equally, if the offence has been committed outside the UK, not only is it likely to be harder to identify the offender, but there would also be complications introduced by the collaboration necessary between the police forces of different nations and by the discrepancies between the laws of the respective jurisdictions.⁶³

Given these issues, it is hardly surprising that official crime statistics are regarded as representing only the tip of the iceberg of the totality of criminal behaviour and that cybercrime in particular is massively under-reported.

⁶² DTI *Information Security Breaches Survey 2004* at

http://www.pwc.com/images/gx/eng/about/svcs/grms/2004Technical_Report.pdf

⁶³ Since something which is a crime in the UK may not be a crime in the nation where it was committed.



In the absence of official cybercrime statistics, it must be acknowledged, as in previous reports⁶⁴, that estimating and quantifying cybercrime is an inherently imprecise activity. This report has drawn on a variety of sources concerned with the selection of available literature on cybercrime. The bibliographic framework explored comprised books, journal articles, 'grey' literature (such as conference proceedings and newspapers),⁶⁵ official publications⁶⁶ and official and unofficial statistics.

Where possible, statistics were derived from interview surveys. Such interviews can provide a better reflection of the true extent of cybercrime because they encompass crimes that are not reported to the police. The British Crime Survey is particularly useful since it does not depend on police recording practices or mechanisms of crime reporting. It therefore provides a more reliable indicator of trends in crime over time.

⁶⁴ UK Cybercrime Reports 2007 and 2008, both published by Garlik

⁶⁵ Auger, C, *Information Sources in Grey Literature* (4th edn, Bowker-Saur, London, 1998).

⁶⁶ Butcher, D, *Official Publications in Britain* (Bingley, London, 1991).

Appendix B – Definitions

Identity theft and identity fraud

Identity theft and identity fraud are not offences in their own right. They are terms that have passed into common parlance to describe the appropriation of some or all of another's identity information, generally with the aim of using the victim's identity as a mask for their own wrongdoing or to evade responsibility for some action or event although there are situations in which another's identity is assumed for innocuous, or at least non-criminal, reasons. In essence, identity theft is the assumption of another's identity irrespective of the motivation for which this course of action is undertaken. It is categorised as a cybercrime despite not being an offence *per se* on the basis that it is frequently the first step that is taken towards the commission of an offence. This first step may be taken because with chosen offence cannot be committed without impersonation of the victim, *i.e.* financial fraud in which the offender passes himself off as the victim, or because the offender is using the victim's identity to shield himself from the consequences of his criminal behaviour, *i.e.* he commits an offence whilst posing as the victim. Irrespective of which of these motivations is operative, the initial first step – the assumption of another's identity – is integral to the commission of the criminal offence that is planned hence the inclusion of identity theft/fraud as a cybercrime is justified as it is a way of facilitating the commission of an offence.

Financial fraud

This category of offences can be defined as the use of deception for direct or indirect financial or material gain. The deception often involves a misrepresentation of the identity of the person concerned, *i.e.* the offender impersonates the victim in order to gain access to things to which the victim is entitled or to incur financial liability in the victim's name. Direct financial gain commonly involves the impersonation of the victim in order to obtain his money, obtain credit in his name or abuse credit facilities that have been granted to him whereas indirect financial gain might involve the assumption of identity information that secures the offender access to more lucrative employment opportunities. This category of conduct is covered within the Fraud Act 2006. The categorisation of these offences as a cybercrime rests on either the commission of the offences online, *i.e.* an online loan application or online shopping, or the use of online resources to facilitate fraud in the physical realm, *i.e.* the acquisition of identity information to make the impersonation of the victim possible and convincing or the creation of a sham online website that purports to offer goods for sale.

Online harassment

The common theme to this category of offences is that the computer is used as a means by which an individual is caused some form of personal harm. Obviously, the remote nature of computer communications precludes any possibility of direct physical harm but there is potential to cause anxiety, distress and psychological harm by indirect means. This may include adverse communications aimed at the victim, *i.e.* abusive or threatening emails, or it may involve communications with a third party – either targeted individuals or the world at large – that are intended to disseminate derogatory or unfavourable information about the victim, *i.e.* false accusations are posted on a website. Alternatively, the offender may use the anonymity offered by the Internet to engage in offensive behaviour whilst posing as the victim thus incurring the wrath of others that will spill into the victim's physical world. The opportunity offered by the Internet to distance oneself from one's words is seen by some as an invitation to bully, harass and threaten others with impunity as one's true identity is shielded. This type of behaviour could give rise to liability for harassment, blackmail, common assault or defamation.

This umbrella category of offences also includes 'hate crimes': the intimidation of a person or group on the basis of their actual or perceived membership of the targeted group. This commonly involves groups associated with particular religious or political beliefs as well as those concerned with sex, race or sexual orientation. It would include abuse directed at victims as well as unfair, untrue, unfavourable or otherwise derogatory information disseminated about those viewed as members of the target group.

Computer misuse

This category of offences is reserved for conduct that falls within the parameters of the Computer Misuse Act 1990⁶⁷ and covers situations such as hacking,⁶⁸ the spread of computer viruses,⁶⁹ and unauthorised access with ulterior intent.⁷⁰

Sexual offences

This category covers a range of conduct that has an objectively ascertainable sexual element, *i.e.* it would be considered by the objective observer to involve sexual wrongdoing irrespective of the subjective views of the parties themselves.⁷¹ This covers paedophilic activity such as grooming a child for sexual activity which was criminalised by the Sexual Offences Act 2003.⁷² The ease of transfer of information offered by the internet and its largely unregulated nature makes it a useful device for those engaged in these sort of offences.

Land registry

This category covers concerns that organised criminals have used the Land Registry to transfer ownership of a property fraudulently – to sell it or apply for a large mortgage secured on the property – without the owners' knowledge.

⁶⁷ Note that amendments to these offences were made by the Police and Justice Act 2006, although the relevant provisions of that Act are not currently in force.

⁶⁸ Computer Misuse Act 1990, s 1.

⁶⁹ Computer Misuse Act 1990, s 3.

⁷⁰ Computer Misuse Act 1990, s 2.

⁷¹ That is, it would be considered by the objective observer to involve sexual wrongdoing irrespective of the subjective views of the parties themselves.

⁷² Meeting a child following sexual grooming, Sexual Offences Act 2003, s 15.

Appendix C - References

APACS, 'Fraud the Facts 2009' <http://www.apacs.org.uk/resources_publications/documents/FraudtheFacts2009.pdf>

Auger, C, *Information Sources in Grey Literature* (4th edn, Bowker-Saur, London, 1998).

BBC News, 'How a fraudster "stole our house"' (31 March 2009).

BBC News, 'Land register "too open to fraud"' (30 March 2009).

British Crime Survey additional report: Mobile phone theft, plastic card and identity fraud: Findings from the 2005/06 British Crime Survey (Supplementary Volume 2 to Crime in England and Wales 2005/06) (15 May 2007)

Butcher, D, *Official Publications in Britain* (Bingley, London, 1991).

CIFAS '2007 Fraud Trends' <www.cifas.org.uk/default.asp?edit_id=790-57>.

CIFAS '2008 Fraud Trends' <www.cifas.org.uk/default.asp?edit_id=896-57>.

DTI *Information Security Breaches Survey 2004* at
http://www.pwc.com/images/gx/eng/about/svcs/grms/2004Technical_Report.pdf

Ellison, L and Akdeniz, Y, 'Cyber-stalking: the Regulation of Harassment on the Internet' (1998) *Criminal Law Review Special Edition: Crime, Criminal Justice and the Internet* 29.

Experian, 'Victims of fraud dossier, Part IV' (May 2008)

Facebook - <http://www.facebook.com/press/info.php?statistics>

Finch, E. (2009) 'Strategies of Adaptation and Diversification: the Impact of Chip and PIN Technology on the Activities of Fraudsters (forthcoming).

Hansard HC Deb (2008-09) VWA 1102 W *(15 May 2009).

Harvey, D, 'Cyberstalking and Internet Harassment: What the Law can Do' (Netsafe II: Society, Safety and the Internet Conference Proceedings, 2003) available at <www.netsafe.org.nz/downloads/conference/netsafepapers_davidharvey_cyberstalking.pdf>

Home Office Statistical Bulletin, Crime in England and Wales 2008/2009; Volume 1, Findings from the British Crime Survey and Police Recorded Crime, 85.

Information Security Breaches Survey Technical Report conducted by PWC and found out [www.pwc.co.uk/pdf/BERR_ISBS_2008\(sml\).pdf](http://www.pwc.co.uk/pdf/BERR_ISBS_2008(sml).pdf)

Kennedy, S, 'Recession will bring big rise in crime and race hatred, says Home Office' *The Times* (1 September 2008)

Maxwell, A, 'Cyberstalking' (Auckland University Department of Psychology, June 2001) available at <www.netsafe.org.nz/ie/downloads/cyberstalking.pdf>.

National Statistics (26 August 2009) <http://www.statistics.gov.uk/CCI/nugget.asp?!D=8>

National Statistics, 'Internet Access 2008' <http://www.statistics.gov.uk/pdfdir/iahi0808.pdf>

'National Campaign Launched to Get UK Safe Online' <http://www.getsafeonline.org/nqcontent.cfm?a_id=1432#_edn1> (October 2005).

Theft Act 1968, s4(1)

The Register, 'Land Registry denies ID fraud risk' (15 August 2007)

The 2001 Internet Crime Forum (ICF) report

Verisign,

<[http://www.imrg.org/8025741F0065E9B8/\(httpPressReleases\)/OCD9C082DE9B46B480257633003D2E08?OpenDocument](http://www.imrg.org/8025741F0065E9B8/(httpPressReleases)/OCD9C082DE9B46B480257633003D2E08?OpenDocument)>

(September 2009)