Home Office

Cyber crime: A review of the evidence

Research Report 75

Chapter 2: Cyber-enabled crimes - fraud and theft

Dr. Mike McGuire (University of Surrey) and
Samantha Dowling (Home Office Science)

October 2013

Cyber crime: A review of the evidence

Chapter 2: Cyber-enabled crimes - fraud and theft

Home Office Research Report 75

October 2013

Dr. Mike McGuire (University of Surrey) and Samantha Dowling (Home Office Science)

Acknowledgements

With thanks to: Andy Feist, Angela Scholes, Ian Caplan, Justin Millar, Steve Bond, Jackie Hoare, Jenny Allan, Laura Williams, Amy Everton, Steve Proffitt, John Fowler, David Mair, Clare Sutherland, Magali Barnoux, Mike Warren, Amanda White, Sam Brand, TSIP, Prof. Majid Yar, Dr.Steve Furnell, Dr. Jo Bryce, Dr Emily Finch and Dr. Tom Holt.

Disclaimer

The views expressed in this report are those of the authors, not necessarily those of the Home Office (nor do they represent Government policy).

Contents

Cyber crime: A review of the evidence
Chapter 2: Cyber-enabled crimes - fraud and theft

What are cyber-enabled crimes?

Cyber-enabled crimes are traditional[1] crimes, which can be increased in their scale or reach by use of computers, computer networks or other forms of information communications technology (ICT). Unlike cyber-dependent crimes, they can be committed without the use of ICT. Two of the most widely published instances of cyber-enabled crime relate to fraud and theft.

Main forms of cyber-enabled fraud

Various forms of cyber-enabled frauds are considered in this chapter.

- *Electronic financial frauds*, most notably *online banking frauds* and *internet-enabled card-not-present (CNP) fraud*. Internet-enabled CNP fraud involves transactions conducted remotely, over the internet, where neither cardholder nor card are present. Related to this are *e-commerce frauds,* which refer more generally to fraudulent financial transactions related to retail sales carried out online. Both businesses and customers may be victims.
- *Fraudulent sales through online auction or retail sites* or through bogus websites, which may offer goods or services that are not provided. Alternatively buyers may be led to purchase a *counterfeit product* (when led to believe it was an original). This may also include other *retail misrepresentations,* such as online ticketing fraud.
- *Mass-marketing frauds and consumer scams*, including advance fee scams such as the 419[2] frauds, inheritance frauds, fake charity or disaster relief frauds, fake lotteries and pyramid schemes. Individuals are persuaded to part with money upfront, for example, to help someone or to invest in a business, on the promise that a larger sum of money will be returned to them at a later date.
- *Phishing* scams are a particular kind of mass-marketing fraud: they refer specifically to the use of fraudulent emails disguised as legitimate emails that ask or 'fish' for personal or corporate information from users, for example, passwords or bank account details. Phishing attempts can be sent out en masse to a range of potential targets, but in the case of *'spear-phishing'* (see *case-study 1*), attackers may gain specific information about a target and tailor communications accordingly to increase the chances of success.
- *Pharming* occurs where a user is directed to a fake website, sometimes from phishing emails, to input their personal details.
- '*Online romance' (or social networking/dating website) frauds*. Individuals may be contacted via social networking or dating sites and persuaded to part with personal information or money following a lengthy online 'relationship'.

[1] 'Traditional' crimes are regarded as those typically recorded within Home Office police recorded crime and are generally thought of as committed in offline environments, for example, fraud, theft, sexual or harassment offences.

[2] The 419 frauds are named after the 419 section in Nigerian legislation, which prohibits this activity. The 419 scams are a form of advance fee scam and have traditionally been linked with Nigerian nationals, but are also committed by other nationalities.

Case-study 1

Spear phishing: A case-study

Customers of a telecommunications firm received an email explaining a problem with their latest order. They were asked to go to the company website, via a link in the email, to provide personal information – like their dates of birth and Social Security numbers. Both the email and the website were bogus.

Instead of casting out thousands of emails randomly hoping that a few victims will bite, spear phishers target select groups of people with something in common – they work at the same company, bank at the same financial institution, attend the same college, or order merchandise from the same website. The emails are ostensibly sent from organisations or individuals the potential victims would normally get e-mails from, making them even more deceptive.

Federal Bureau of Investigation, 2009

Main forms of cyber-enabled data theft

Cyber criminals may seek to obtain personal and financial data for fraudulent purposes. Cyber-enabled data theft is therefore an integral part of any discussion on fraud. Valuable forms of data may include:

- personal information (names, bank details, and National Insurance numbers);
- company accounts;
- client databases; and
- intellectual property (for example, new company products or innovations).

Victims may be members of the general public or businesses.

The main methods and techniques involved in cyber-enabled data theft include the following:

- *Use of technology to steal personal data* – this includes hacking, keylogging[3] and other techniques designed to exploit vulnerabilities in computer systems or networks. These are outlined further in Chapter 1: Cyber-dependent crime.
- *Detailed online searching for personal information* – this includes searching for dates of birth, names and family details, all of which are now regularly stored on social networking, directory, dating and employment websites. Other sites can be used to work out a person's identity. Such information can be used, for example, to access bank accounts and e-mails, or to allow specific targeting with phishing emails.
- *Social engineering techniques* – these play on the basic premise that most people trust others online and users can be deceived or duped into parting with personal information or money. These are key to common frauds, such as phishing emails. Cyber criminals may use fear, authority or other persuasive tactics and may combine social engineering with other techniques such as pharming, to obtain personal details or money.

Given that online transactions are not conducted face to face, methods of guaranteeing trust in an individual's identity – i.e. that someone is who they claim to

[3] Keylogging captures and forwards typed input from a machine, enabling collection of sensitive data such as passwords or bank accounts.

be – have become increasingly important (Smith, 2006). As a result, the fabrication and misuse of identity-related data has become as notable a feature of the cyber-enabled fraud landscape as fraud itself. Terms such as 'identity fraud' or 'identity theft' are often treated interchangeably with fraud and this overlap in terminology is one of many factors creating ambiguities when estimating the scale of cyber-enabled fraud.[4] There are important distinctions between fraud, identity-related theft and the techniques used to obtain personal details, such as phishing or hacking. These may be distinguished as follows:

- the theft of personal details and the techniques used to undertake the theft (this may involve phishing or hacking, for example);
- the sale of stolen identification (for example, in online forums);
- the use of stolen identification to commit fraud; and
- the fraud itself.

Key findings: What is known about cyber-enabled fraud and theft?

Scale and nature of cyber-enabled fraud

Victimisation surveys

Experiences of financial loss online, mass-marketing frauds, phishing emails and other scams are reported in various surveys of the public and businesses. The most robust of these and conducted on a regular basis are the Crime Survey for England and Wales (CSEW; for example, see ONS, 2012) and surveys by the Oxford Internet Institute (Dutton and Blank, 2013) and OfCom (2013). One-off surveys have also been conducted by Ipsos MORI (2013) and the ONS (2010). Amongst businesses, one of the most robust surveys available is the Commercial Victimisation Survey (CVS; Home Office, 2013a).

However, as for cyber-dependent crimes, most of these surveys capture information on internet users' negative online experiences. They do not measure criminal activity or police recorded crime. So whilst they can be useful indicators, they do not give firm measures of prevalence for cyber-enabled (or cyber-dependent) crimes. It is unlikely that many of the incidents recorded in these surveys would meet the specific criteria to be classified as a 'crime' under Home Office Counting Rules[5] (HOCR, see also p 13).

[4] There are various terms used to describe identity-related frauds/theft. McQuade (2006) defines identity theft as *"acquiring and then unlawfully using personal and financial account information to acquire goods and services in someone else's name"* (p 69). However, the term can be misleading since, literally speaking, an individual's identity can never be stolen. Rather it is identification data (such as banking details) that are stolen and used to impersonate individuals. McGuire (2007) instead characterises identity theft as 'identification theft'.

[5] For example, these incidents would have to meet the Home Office 'specific intended victim' rule, which is a key determinant in distinguishing between an actual crime and a crime-related incident under Home Office Counting Rules (HOCR). HOCR state, for example, that 'attacks' should not be recorded as crimes. Where people are cold-called or receive global emails as part of a mail shot, they are not generally specific intended victims. Something has to happen as a result, i.e. the victim has to take action following the initial contact. This could be: a specific communication with the offender; a click on a link to a fake website in a phishing email; or actions that lead to a financial loss occurs (but these incidents do not have to involve a loss).

Public experiences of cyber-enabled fraud and theft

A summary of key findings from surveys of financial loss, cyber-enabled retail fraud and identity fraud amongst the general public are outlined in Table 2.1.

Overall, victim-based surveys suggest that *experiences of financial loss online* amongst the public are relatively low compared with other negative experiences online (see Chapter 1: Cyber-dependent crime). For example, the CSEW (2011/12, see ONS, 2012) reported that 3 per cent of adult internet users had 'lost money' whilst using the internet in the 12 months prior to interview (although it is not known how this loss occurred). Ipsos MORI (2013) found that 5 per cent of internet users had experienced financial loss from credit/debit card misuse online in the 12 months prior to March 2012. The ONS (2010) similarly reported that 3 per cent of adult internet users had experienced financial loss due to fraudulent online card payments in the 12 months prior to interview. However, given that survey questions of this form ask specifically about loss of money, these responses are likely to be an underestimation, given that banks reimburse losses so individuals may not view themselves as 'victims' or having experienced a financial loss.

In relation to *e-commerce or online retail frauds*, victim surveys suggest that nearly 10 per cent of internet users have 'bought something online that was misrepresented'; this proportion remained relatively stable between 2005–11, but rose from 9 per cent in 2011 to 12 per cent in 2013 (Dutton & Blank, 2013). The same survey also reported an increase in the proportion of internet users who have had their credit card details stolen, from three per cent in 2011 to six per cent in 2013. The Eurobarometer (2012) survey reported that 16 per cent of UK adult internet users (aged 15 years and over) reported non-arrival of goods, goods being counterfeit or finding goods were not as advertised. However, there could also be non-criminal reasons for this type of issue, such as failed deliveries or trading standards.

Table 2.1: Summary of findings from surveys of financial loss online, e-commerce and identity frauds.

Survey	Type of fraud	Sample size and methodology	Key findings
Crime Survey for England and Wales 2011/12 (ONS, 2012)	Financial loss online.	8,373 adult internet users, aged 16+.. Random sample of households in England and Wales.	3% lost money whilst using the internet. (In 2010/11, 3% also lost money).
Public Attitudes to Internet Security Survey, (Ipsos MORI, 2013)	Financial loss online.	1,518 adult UK internet users aged 15+. Random locale sampling.	5% experienced financial loss from credit/debit card misuse online.
Oxford Internet Survey (Dutton and Blank, 2013)	E-commerce/online retail frauds.	2,657 British internet users aged 14+. Random sample.	12% bought something online that was misrepresented. 6% had credit card details stolen.
Cyber Security Survey (Eurobarometer, 2012)	E-commerce/online retail frauds and identity fraud.	1,018 UK internet users aged 15+. Random sample.	16% found goods purchased did not arrive, turned out to be counterfeit or were not as advertised. 12% were victims of identity fraud (where someone used personal data to impersonate them).
Findings from Consumer Surveys on Internet Shopping (OFT, 2009)	E-commerce/online retail frauds.	1,938 UK adult internet users.	8% caught by fake or non-existent scam websites. 8% were victims of online ticketing fraud.
Scottish Crime Survey 2010/11 (The Scottish Government, 2011)	Identity theft.	3,250 adults from Scotland. Random sample.	Estimated 0.5% were victims of identity theft (where someone had pretended to be them or used their personal details fraudulently).

Experiences of *'identity fraud'* are often asked about in surveys of fraud. However, it is not a particularly useful measure. There is a lack of clarity amongst the public about what is meant by 'identity fraud' and it can too easily overlap with other terms such as cyber-enabled fraud and plastic card fraud, leading to double counting in many estimates. In an EU-wide survey (Eurobarometer, 2012), 12 per cent of UK respondents reported being a victim of identity fraud. The 2010/11 Scottish Crime Survey estimated that 0.5 per cent of adults have been victims of identity theft, where someone had pretended to be them or used their personal details fraudulently in the past 12 months (The Scottish Government, 2011).

Mass-marketing frauds and consumer scams were traditionally conducted via letter or telephone. However, the advent of email and social networking has broadened their reach. Phishing emails are one particular kind of mass-marketing fraud.

Table 2.2 outlines findings from various victim surveys that have explored the receipt of unsolicited communications, mass-marketing frauds, phishing emails and other scams. Receipt of these types of scams appears to be relatively common, and the proportion of adult internet users experiencing phishing attempts in particular has been increasing. The Oxford Internet Survey reported a statistically significant increase in phishing attempts from 12 per cent in 2005 to 22 per cent in 2011. However, this has since fallen to 19 per cent in 2013 (Dutton and Blank, 2013). The Eurostat (2010) survey placed the UK second (at 7%), behind Latvia (at 8%) in the number of internet users reporting phishing, pharming and payment card losses across the EU.

Table 2.2: Summary of key findings from surveys of experiences of attempted mass-marketing frauds, phishing e-mails and scams.

Survey	Type of mass-marketing fraud/scam measured	Sample size and methodology (where known)	Key findings
Crime Survey for England and Wales 2011/12 (ONS, 2012)	Receipt of potential fraud-related communications (by email, text, letter or phone call).	42,232 adult respondents. Random sample of households in England and Wales.	56% reported receiving one or more potentially fraud-related communication(s). 40% received notification of a big win in a lottery or prize draw that they had not entered. 16% were offered the chance to make an investment with a guaranteed high return. 15% were offered a loan on attractive terms. 13% were invited to get to know someone for a potential relationship/friendship (romance fraud).
Oxford Internet Survey (Dutton and Blank, 2013)	Phishing attempts.	2,657 British internet users aged 14+. Random sample.	19% of internet users had experienced an attempt to acquire their banking details. This was an increase from 12% recorded in 2005, but a decline from 22% in 2011.
Communications Market Report (Ofcom, 2012)	Receipt of unsolicited emails or messages directing to websites asking for personal information.	1,369 UK internet users. Random locale sample.	28% of UK internet users had experienced this type of message.
Cyber Security Survey (Eurobarometer, 2012)	Received scam emails fraudulently asking for money or personal details.	1,305 UK internet users aged 15+. Random sample.	52% experienced a scam email (21% often, 31% occasionally, 48% never).

Whilst many surveys do not ask whether ‘attempts’ were successful or not (and some do not distinguish between online and offline experiences), the available survey data suggest that very low proportions of adult internet users have had financial loss from

such a scam (see Table 2.3). For example, both ONS (2010) and Ipsos MORI (2013) found that three per cent of adult internet users reported financial loss as a result of fraudulent messages or being sent to fake websites asking for information (although it is not known what level of financial loss actually occurred in these cases). This suggests that the public is largely aware of and mostly ignore unsolicited communications and potential online scams. Experiences of loss from scams are also likely to be under-reported as victims may feel embarrassed and not wish to admit that they have been duped.

Table 2.3: Summary of key findings from surveys of financial loss from online mass-marketing frauds, phishing e-mails and scams.

Survey	Type of mass-marketing fraud/scam measured	Sample size and methodology (where known)	Key findings
Internet Access 2010: Households and Individuals (ONS, 2010)	Financial loss from fraudulent messages or being sent to fake websites asking for information.	Approximately 1,200 interviews per month carried out over 4 months in the UK (January-April).	3% experienced financial loss.
Attitudes to Computer Security Survey (Ipsos MORI, 2013)	Financial loss from fraudulent messages or being sent to fake websites asking for information.	1,518 adult UK internet users. Random locale sampling.	3% experienced financial loss.
The online romance scam: A serious cyber crime (Whitty and Buchanan, 2012)	Online romance scams.	2,028 UK adults. Random sample.	Under 1% of the sample reported losing money to online romance scam.
Research on impact of mass-marketed scams (OFT, 2006)	Mass-marketing scams (both online and offline).	11,200 UK adults.	2% reported being a victim.

Business experiences of cyber-enabled fraud and data theft

The 2012 Commercial Victimisation Survey is a key source of data for business experiences of negative online incidents. The results of the CVS are representative of online crime incidents against the four sectors covered (manufacturing; wholesale and retail; transportation and storage; and accommodation and food), but are not representative of businesses as a whole. In addition, the CVS is a premises-based (rather than head office-based) survey and many types of online crime may therefore not be picked up by the CVS as they do not affect businesses at the premises level. In addition, not all incidents reported in the survey would be classed as a crime under Home Office Counting Rules.

Overall, there were relatively low levels of cyber-enabled theft and fraud reported in the 2012 CVS in the 12 months prior to the interview (see Table 2.4). There were 8,000 incidents of online theft of money (1% of all businesses surveyed), 3,000 incidents of information theft and 1,000 phishing incidents. This compared with 135,000 virus incidents recorded across all four sectors (Home Office, 2013a).

Table 2.4: Numbers of incidents of online crime experienced in the last 12 months, by industry sector, 2012 Commercial Victimisation Survey

Number of incidents	Manufacturing ('000s)	Wholesale and retail ('000s)	Transportation and storage ('000s)	Accommo-dation and food ('000s)	All four sectors ('000s)
Hacking	13	7	5	2	27
Phishing	0	0	0	1	1
Theft of money (online)	1	3	3	1	8
Theft of information (online)	0	3	0	0	3
Website vandalism	0	1	0	5	7
Computer virus	64	55	10	8	135
All online crime	**78**	**69**	**19**	**16**	**180**

Source: Home Office (2013a)

Evidence relating specifically to cyber-enabled data theft[6] is limited. It is often difficult to isolate online from offline incidents and measures tend to be conflated with negligence and recorded as 'data loss' rather than a deliberate act of theft. For example, available data from the Information Commissioner's Office (ICO) reported 1,000 data breaches between November 2007 and May 2010 and recent freedom of information (FOI) requests suggest data breaches generally have been increasing in the past five years.[7] However, the term 'data breaches' includes both online and offline incidents, and instances of data loss as well theft (ICO, 2010). [8] Evidence in this area also primarily relates to businesses rather than to members of the public. However, even if a business is the initial victim of data theft members of the public may also be victims, depending on what is stolen and how it is used.

The PwC survey of business security breaches has run annually for a number of years. It is one of the most in-depth surveys of security breaches available, although the methodologies used for the survey have varied over time. Up to 2008 the survey adopted a random probability sampling method and showed that four per cent of businesses surveyed in 2008 experienced theft or fraud using computers, although this also included incidents of physical hardware theft (BERR, 2008). From 2010 onwards, the methodology changed to a self-selecting, non-random sample. The most recent survey (PwC, 2013) found that 47 per cent of large organisations (more than 250 employees) and 16 per cent of small organisations (less than 50 employees) reported a theft or fraud. It is not possible to compare these later figures with the 2008 data.

[6] The term data theft refers to the theft incident itself and not what was done with the data afterwards (for example, used to commit fraud).

[7] See: http://www.bbc.co.uk/news/technology-19424197

[8] The ICO confirmed that whilst information regarding cyber-enabled incidents would be held within individual case files (and could be found through a lengthy manual search), it was not possible to electronically search for criteria relating to cyber-enabled data thefts (personal communication from the ICO, 19 September, 2012). However, an improved data collection system introduced in the ICO from April 2012 will help to identify more easily data breaches relating to technical issues (such as hacking).

Police recorded crime and Action Fraud

Measuring the scale of cyber-enabled fraud and theft faces similar problems to those associated with cyber-dependent crimes.

Police record crime in accordance with the provisions of the HOCR, which set out that the crime to be recorded is determined by the law. Since there is no specific offence (or offences) of cyber crime – aside from those specified in the Computer Misuse Act 1990 – police recorded crime does not generally distinguish between offline and online offences. Whether or not the offence was committed online or offline, is cyber-enabled or cyber-dependent, the offence recorded is on the basis of the offence in law. For example a fraud committed using a computer would usually be recorded as a fraud under police recorded crime. Sentencing data held by the Ministry of Justice also do not identify cyber-enabled offences – prosecutions are made in relation to the offence, not the medium used to commit it.

Before the roll out of Action Fraud as the national reporting centre for fraud and financially motivated cyber crime, computer misuse and fraud offences were recorded by individual police forces. Action Fraud completed rollout in April 2013 and responsibility for recording of all fraud and computer misuse offences has since transferred to Action Fraud. Action Fraud captures reports on these offences from public and businesses and classifies them in a way which allows distinctions to be made between computer misuse, online fraud and offline fraud offences. Action Fraud also assesses them against the provisions of the law and the requirements of HOCR. Where a report falls short of being recorded as a crime under HOCR, Action Fraud has the facility to record it as an incident, for intelligence and information purposes.

Initial Action Fraud data from the rollout period shows that Action Fraud received a total of 47,980 crime and information reports of cyber-enabled enabled fraud between January and December 2012. This comprised 35 per cent of all reports made to Action Fraud during this time. As outlined in Table 2.5, the largest proportion of these were for online shopping and auctions (39%), followed by other advance fee frauds (11%) and computer software service fraud (8%). These new data provide an indication of the type of information now available, although the initial data present only a partial picture as they occur in a transitional period of time when Action Fraud had not yet rolled-out to all forces. Action Fraud was initially rolled out to five forces in January 2012, rising to 24 forces by December 2012 and to all forces by April 2013.

Table 2.5: Number of cyber-enabled frauds reported to Action Fraud, January–December 2012

Cyber-enabled fraud type	Volume	%
Online shopping frauds and auctions	18,701	39%
Other advance fee frauds[9]	5,290	11%
Computer software service fraud	3,577	7.5%
Fraud not counted elsewhere[10]	3,245	6.8%
Ticket fraud	2,929	6.1%
Banking and credit industry fraud	2,155	4.5%
Other consumer non-investment fraud[11]	2,041	4.3%
Dating scam	1,361	2.8%
Lender loan fraud	1,179	2.5%
Counterfeit cashiers cheques	1,124	2.3%
Other	6,378	13.3%
Total	**47,980**	**100%**

Source: Action Fraud (2012)
Note: Figures include reports of crimes and 'information' reports – all are cyber-enabled.

As awareness of the reporting facility increases, it is expected that there will be an increase in reporting, which will be captured in the 2013 data. New Action Fraud figures are already starting to be included in official recorded crime statistics and this showed there were 229,018 fraud offences recorded in total in the year ending March 2013. This represents a volume increase of 27 per cent compared with the previous year. Whilst it is possible this could mean there has been some increase in fraud, the ONS (2013) state that there are a number of factors that could have contributed to this increase - notably the centralisation of recording fraud within Action Fraud, a possible improvement in recording practices and an increased proportion of victims reporting fraud following publicity around the launch of Action Fraud. In the context of the move to centralised recording of fraud from local police to Action Fraud, making comparisons over time is problematic.

The HOCR govern whether an incident reported to Action Fraud is counted as a crime. The general rule relates to whether the individual concerned was a 'specific intended victim'. Under this rule it is not sufficient, for example, to have simply received a phishing email for a crime to be reported for statistical purposes. The victim needs to have taken some action following the initial contact from the offender, in order to make them a specific intended victim. For example, communicating with the offender, clicking a link, or suffering some resulting loss from the phishing email.

Further details surrounding HOCR for cyber-dependent crimes are outlined at www.gov.uk/government/uploads/system/uploads/attachment_data/file/210800/count-fraud-april-2013.pdf.

[9] Other Advance Fee Fraud refers to advance fee frauds that do not fall under other categories such as 419 frauds. For example: 'Mr A' has advertised his car for sale online. He is emailed by someone saying that they have a buyer for his car. If he pays them £100 he will put them in touch with him. 'Mr A' transfers £100 to an account that was provided but hears nothing further. The person who made contact never had any details of any buyer for the car.

[10] 'Fraud not counted elsewhere' contains a mixture of frauds that do not fit into any other Home Office counting rule categories. For example, this category includes situations where victims have been contacted by 'friends' via social media sites and lured into get-rich-quick schemes. These schemes do not fall within the investment fraud categories and therefore are considered 'fraud not counted elsewhere'.

[11] Refers to other consumer non-investment fraud not counted in other categories. For example, the police are called to an airport where five passengers have purchased holidays over the internet. On arrival at the airport they discover that the company does not exist and there is no holiday.

Industry sources

The majority of private sector and industry evidence regarding the extent of online banking, plastic card fraud and e-commerce frauds tends to relate to financial losses to the banking/payment sector rather than measures of prevalence. These data are outlined on pp 16-17.

In relation to phishing, industry sources also suggest that phishing attempts are rising in the UK. Financial Fraud Action, for example, reported 51,161 phishing websites directed against UK banks in 2009, increasing to 256,641 reports in 2012[12] (Financial Fraud Action, 2013). At a global level, security providers such as RSA have reported spikes in the number of unique phishing attempts recorded within their own customer base.[13] It is not known, however, what level of loss occurred with these attempts or if they were successful.

The Anti-Phishing Working Group (APWG) collates reports of unique phishing emails and websites reported by its members and the public through its website and also through research partners. The APWG suggests that most attacks appear to originate from outside the UK and that the UK is typically found to host a much smaller proportion of phishing sites than other countries. During 2012 the highest proportion of phishing sites hosted by the UK peaked at just over four per cent, in October 2012 (APWG, 2013). In comparison, the US consistently hosted the largest proportion of phishing sites – nearly 88 per cent of phishing sites reported to APWG in May 2012. The UK hosted 0.44 per cent in the same month (APWG, 2012).

The security provider RSA (2012) similarly reported few phishing sites hosted by the UK (3% in August 2012). RSA also found that the UK was the top country targeted from March through to August, accounting for 70 per cent of all phishing attempts recorded in August 2012. The US and Canada were second (23%) and third (6%) in terms of countries attacked.

Characteristics of victims

The general public

Similar proportions of men and women internet users experienced loss of money in the last year – both three per cent according to the Crime Survey for England and Wales 2011/12 (ONS, 2012). Women aged 65 and over were least likely to have experienced loss of money while using the internet (1% of those aged 65 to 74 years and 0% of those aged 75 and over).

For comparisons with other types of negative online experiences, please see p 7 in Chapter 1: Cyber-dependent crime.

The National Fraud Authority (NFA) has explored vulnerabilities amongst individuals for online and offline frauds in order to help to inform awareness campaigns. In 2011 the NFA surveyed 2,062 members of the general public (a non-random sample) regarding their experiences of fraud. It then categorised fraud victims into various 'segments', relating to their demographics, behaviours, attitudes and overall

[12] Although it is not clear how much of this relates to increases in awareness/availability for reporting and how much is due to an actual increase.
[13] For example, the rise from 19,141 reported attacks in February 2012 to 59,406 in July 2012 was attributed to increased activity against the RSA's European banking customers.

vulnerability in relation to fraud (National Fraud Authority, 2011). Whilst the segmentation covered fraud in general, many of the experiences and attitudes also related to online fraud. There were seven types of victims identified:

- segment 1 – those avoiding risk but lacking awareness;
- segment 2 – those avoiding risk and demonstrating exemplary behaviour;
- segment 2b – those avoiding risk but vulnerable to offers;
- segment 3 – those avoiding risk but still a victim;
- segment 4 – risk takers seeking financial gain;
- segment 5 – risk takers demonstrating naivety;
- segment 6 – risk takers and sure of themselves; and
- segment 7 – risk takers with poor behaviour.[14]

The analysis was designed to help to inform future awareness-raising and education campaigns targeted specifically at different types of victims, such as the 'Devil's in your Details' campaign (Action Fraud, 2013).

Businesses

According to the 2012 CVS, there were no clear differences in terms of business size in relation to experiences of online 'crimes' - both large and small businesses reported being victims. It reported that 11 per cent of businesses with 50 or more employees had been a victim of one or more online crime incidents, compared with 9 per cent of those with 10–49 employees and 8 per cent with 1–9 employees (Home Office, 2013b).

Table 2.6: Proportion of business premises that experienced online 'crime' in the last 12 months, by size, 2012 Commercial Victimisation Survey

	1–9 employees (%)	10–49 employees (%)	50+ employees (%)	All four sectors[1] (%)
Hacking	2	2	2	2
Phishing	0	0	0	0
Theft of money (online)	1	0	0	1
Theft of information (online)	0	1	0	0
Website vandalism	0	1	1	0
Computer virus	7	7	10	7
All online 'crime'	**8**	**9**	**11**	**8**
Unweighted base	946	559	492	1,997

Source: Home Office (2013b)
Note: The four sectors are: wholesale and retail; manufacturing; transportation and storage; and accommodation and food.
Note2: The percentages under "All online 'crime'" will not add up to total figures presented in graph due to the survey methodology used. As opposed to counting each individual incident of online crime once, this survey grouped all incidents together as "one or more".

[14] See: http://www.homeoffice.gov.uk/publications/agencies-public-bodies/nfa/national-fraud-segmentation?view=Binary

Estimating the costs of cyber crime

Estimating the costs of cyber crime is challenging. Chapter 1: Cyber-dependent crime outlines the research available on this topic more generally (for example, Detica, 2011; Anderson *et al.*, 2012). Otherwise, the majority of evidence on costs regarding cyber-enabled fraud relates to costs to the banking/payments sector and is generated by the finance sector.

Online banking, plastic card and e-commerce frauds

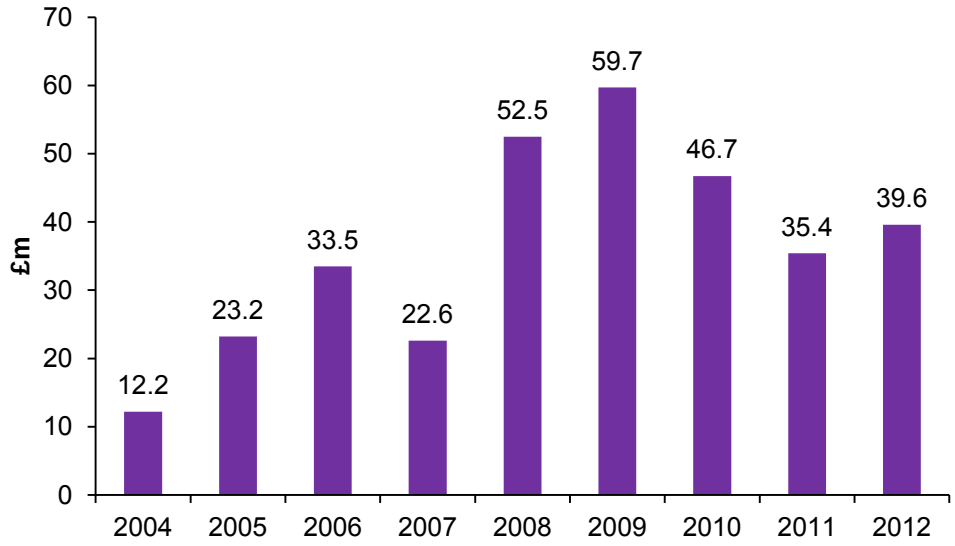
Costs to the banking and payments industry sector

Financial Fraud Action (2012; 2013) provides regular reports on losses to the banking/payments card sector from various forms of fraud. These reports are collated from information provided by the banks regarding details of all their actual fraud cases and associated losses, in line with the agreed industry definitions and categories.

The most clearly defined forms of cyber-enabled fraud relate to costs from online banking and internet-enabled card-not-present frauds.

Online banking frauds involve the misuse of online banking facilities, for example, attempts to fraudulently access customer accounts and divert funds from them. Losses from online banking fraud have been declining since 2009 (see Figure 2.1). However, Financial Fraud Action (2013) reported £39.6 million in losses to the banking/payments sector from this form of fraud in 2012, a 12 per cent increase from 2011.

Figure 2.1. Costs from online banking fraud, 2004 to 2012

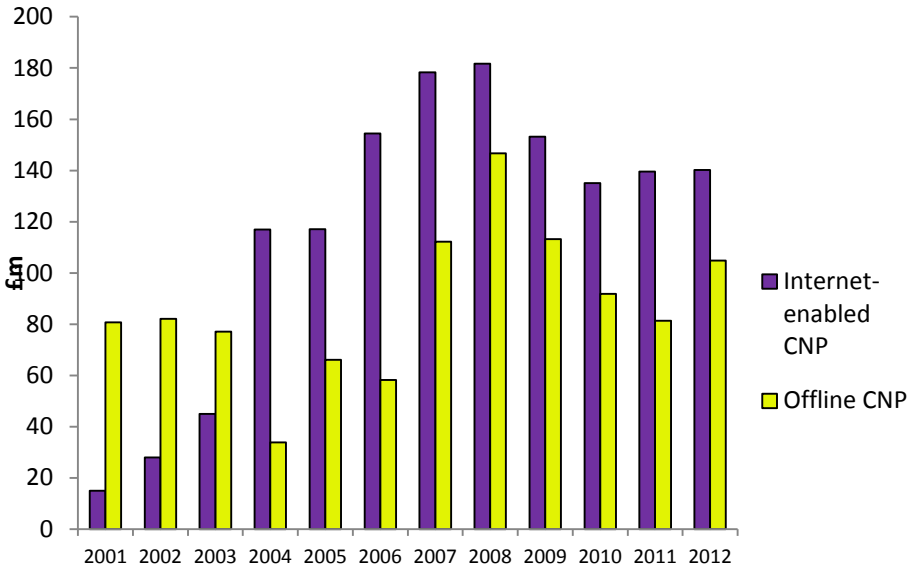


Source: Financial Fraud Action (2013)

Card-not-present (CNP) fraud involves transactions conducted remotely (i.e. on the internet, by telephone or mail order) where neither the cardholder nor card are present. Figure 2.2 shows the value of internet-enabled CNP fraud and offline (for example, by telephone) CNP fraud from 2001 to 2012. Losses to the banking system *from internet-enabled CNP* (also described by Financial Fraud Action as 'e-

commerce fraud') increased rapidly in the early 2000s with the growth of internet shopping, but have fallen since 2008. Losses from this form of fraud increased by less than 1 per cent between 2011 and 2012, from £139.6 million to £140.2 million. Overall, losses from both offline and internet-enabled CNP fraud to the banking/payments sector increased by 11 per cent between 2011 and 2012, reaching £245.8 million in 2012. The proportion of CNP fraud that was internet-enabled was 57 per cent in 2012, down from 63 per cent in 2011 (Financial Fraud Action, 2013).

Figure 2.2. Costs of card-not-present fraud, internet-enabled and offline, 2001 to 2012



Source: Financial Fraud Action (2013)

Overall, total losses from *plastic card fraud* (including cyber-enabled and offline frauds) saw year on year declines from 2008 to 2011. Then there was an increase of reported losses from £341 million in 2011 to £388 million in 2012.

Reductions in costs from both online banking fraud and internet-enabled CNP fraud are likely to be due to the introduction of security measures such as Chip and Pin, American Express SafeKey, Mastercard Secure Code and Verified by Visa, which require users to enter a password when purchasing from retailers participating in the schemes (Financial Fraud Action, 2012). Anderson *et al.* (2012), however, claim that the reduction in losses from fraud to the banking/payments industry sector is not only due to the technical aspects, but is also a result of *"more vigorous dumping of liability on merchants and card holders"* (p 8).

A particular challenge when considering evidence regarding the scale and cost of cyber-enabled fraud, relates to the variety of alternative and often overlapping fraud/cyber-enabled fraud categories and definitions used across different sources.[15] 'Identity frauds', for example, can easily overlap with cyber-enabled frauds and it is hard to distinguish these from plastic card or CNP frauds, which can both potentially be classed as identity fraud or cyber-enabled. Authors such as Anderson *et a*l. (2012) suggest that for some frauds *"doubt remains over whether they should be*

[15] Other well-known sources for traditional fraud estimates, such as CIFAS (the UK's fraud prevention service), include a range of different categories to Financial Fraud Action.

considered – at least partly – to be cyber crimes or not" (p 11). Once a card has been lost or stolen 'offline', it can be used fraudulently online, for example, as part of an internet CNP fraud. It is not clear though how many cards reported as lost or stolen (to Financial Fraud Action, for example) may have been used in this fashion, or what the potential is for double-counting between categories. Furthermore, common methods for committing fraud can be technical in nature (for example, ATM skimmers) and the majority of card transactions in the UK are authorised online and use EMV[16] (Anderson *et al*., 2012), so may also be considered as digital frauds.[17] Other cost estimates within research in this area therefore include other types of fraud, for example, Anderson *et al.* include estimates of Private Automatic Branch Exchange (PABX) fraud.[18]

Costs to the retail sector

The estimates of losses reported by Financial Fraud Action relate to just the banks/payments industry and not the retail sector, or the public. Furthermore, Financial Fraud Action only uses internet-enabled CNP fraud as a measure of 'e-commerce fraud', but a more complete measure of e-commerce might also include other digital payments systems, such as PayPal.

The British Retail Consortium (BRC, 2012) attempted to address knowledge gaps regarding costs of 'e-crime' to the retail sector by surveying UK retailers that, it stated, were responsible for 45 per cent of online UK retail sales. BRC estimated total losses of over £205 million in 2011–12. This estimate largely focused on losses from e-commerce frauds, as retailers were unable to estimate losses from cyber-dependent crimes. The estimate comprised £77.3 million in direct losses (most notably, identification-related frauds, card and CNP frauds, and refund frauds), £16.5 million in security costs and £111.6 million in estimated lost revenue from online fraud prevention (caused by online security measures driving away legitimate purchases).

However, it is difficult to estimate such losses accurately. Many of the survey-based estimates of loss that have been undertaken to date are likely to represent just a fraction of the individuals/organisations surveyed and may be skewed upwards by extreme losses reported by a few respondents.

Mass-marketing frauds and consumer scams

There are no reliable data available for financial losses to the UK from mass-marketing frauds/scams. Available evidence on costs for mass-marketing frauds and scams tend to be based on anecdotal evidence of individual cases, *"with what figures there are being a summation of all cases … and perhaps multiplied up to speculatively account for under-reporting"* (Anderson *et al.*, 2012). Anderson *et al.* state that they had no real evidence to support their own estimate of losses to the UK from advanced fee fraud and picked a number ($50 million) to *"avoid a gap in our table"* (p 16). (Anderson et al. were able to provide case study evidence for other

[16] EMV stands for 'Europay, Mastercard & Visa' – the global standard for the inter-operation of chip cards, point of sale terminals capable of taking these cards, and ATMs, for authenticating credit and debit cards.

[17] Arguably, if one's definition of cyber-enabled fraud also includes 'any digital network', then telephone banking may also be captured within such a definition (McGuire, 2012).

[18] PABX fraud occurs where a criminal reconfigures a company (or individual's) telephone system (mobile or fixed) to accept incoming calls and relay them onwards at the company/individual's expense. PABXs are now often placed on the internet.

aspects of cyber crime though, see Chapter 1: Cyber-dependent crimes for further discussion on costs of cyber crime).

Cyber-enabled data theft

There are no reliable estimates of the cost of data theft to either UK companies or members of the public.

Ponemon Institute (2012) estimated costs of approximately £2 million in 2012. However, Ponemon's research draws from 38 case-study organisations, that had each experienced an average of 23,833 breached records, and these are unlikely to be representative of wider businesses.

Detica (2011) estimated costs of customer data loss to businesses to lie between £0.96 billion and £1.44 billion[19] and the costs of online theft to lie between £1 billion and £2.7 billion. Although, as the report states – the online data theft estimate is based on *"broad assumptions…in the absence of data being available on the actual level of online data theft"* (p 21).

The same report (Detica, 2011) also estimated losses of £7.6 billion per annum resulting from industrial espionage and £9.2 billion to intellectual property theft. Anderson *et al.* (2012) declined to offer an estimate for this form of cyber crime in their own research, arguing that there was *"no obvious foundation"* (p 17) for the Detica estimates and no credible figures available for espionage.

The most recent attempt to calculate losses from data loss/theft to members of the public was by the National Fraud Authority (2013) for the Annual Fraud Indicator, drawing on a survey of 4,000 individuals. The survey found that around 9 per cent reported being a victim of identity theft and the average loss per victim was £1,203, leading the National Fraud Authority to estimate the average loss to the UK as around £3.3 billion in 2013. However, extrapolating losses from surveys in this way is problematic, as losses are based on unverified self reports, where single outliers can heavily skew and exaggerate results. A large proportion of the estimate can often come from just a handful of the respondents (as distribution of losses amongst the population is not likely to be experienced in a uniform manner).[20]

The broader challenges associated with estimating the costs of cyber crime are discussed in Chapter 1: Cyber-dependent crime.

Non-financial impacts

Since most fraud victims would expect to get money back from their bank, it seems plausible that financial impacts on victims may be short-lived. By contrast, the wider and long-term impacts of cyber-enabled fraud and identity-related theft are far less well explored. Impacts such as poor credit ratings or loan rejections may not materialise until an individual applies for a loan. For example, US research has found that victims may experience issues such as harassment by creditors or criminal investigations following the fraudulent use of their data (Federal Trade Commission, 2006).

[19] They did this by combining the same data from the aforementioned Ponemon Institute (2012) and supplementary data from the Department for Business, Innovation and Skills (BIS)/Department for Trade and Industry (DTI) information security breaches reports from 2004.
[20] For further details on this issue see Florencio and Herley (2011).

A (non-random) survey of internet users by Get Safe Online (2012) reported that of the 1,764 individuals who had experienced some form of cyber crime, 19 per cent lost money as a result, but others also reported: having to change all their passwords (41%); replace all their bank and credit cards (15%); set up new email accounts (13%); and generally waste a lot of time fixing problems (38%). Just under one fifth (18%) also experienced embarrassment. Primary research amongst victims of scams by the Office of Fair Trading (OFT, 2009) also outlined the embarrassment and in some cases, severe loss of self-esteem felt by victims.

Recent research from the Sentencing Council (Kerr *et al.*, 2013) also outlines potential psychological or emotional harms from two specific fraud offences – confidence fraud and the possessing, making or supplying articles for use in fraud. This study found that, aside from the financial impacts, fraud can cause victims psychological and emotional harm (such as anxiety, anger, stress, depression and self-blame), and can damage their relationships, making it difficult for them to trust others. In some cases victims were left feeling physically threatened (for example, fearing that the perpetrator might go to their house), and changed their behaviours in the long-term (for example, by no longer shopping online, causing inconvenience).[21]

Despite concerns over personal details and online security, consumer online confidence appears to be growing and users continue to shop and transact online. For example, the OFT found that the proportion of online shoppers with no concerns more than doubled, from 12 per cent in 2006 to 28 per cent in 2009 (OFT, 2006). An increased proportion also felt online shopping was as safe as shopping in store, rising from 26 per cent in 2006 to 54 per cent in 2009 (OFT, 2009). Of the online shoppers who did have concerns (n=332), the majority (68%) were concerned about security issues (financial details being divulged), but this figure had also declined in 2009 (by 10 per cent since 2006).

Characteristics of offenders

There is limited published evidence available regarding offenders linked to cyber-enabled fraud and data theft. Whilst topics such as insider-enabled cyber crimes and organised cyber crime have been the subject of much discussion in recent literature, there is little high-quality evidence available on the extent of the problem. As with cyber-dependent crimes there are knowledge gaps around offender characteristics, their backgrounds and career pathways, and the links between online and offline offending.

The Home Office Offending, Crime and Justice Survey (OCJS) provides some insight into the characteristics of cyber-dependent and cyber-enabled offenders. The survey was the first and only nationally representative survey of self-reported offending carried out every year between 2003–06 and includes questions on self-reported technology offending (Allen *et al*., 2005). Despite the survey now being quite dated it can help to fill some knowledge gaps in this area. However, it should be noted that not all of the offending behaviours included in the survey necessarily relate to criminal activity (and classed as a crime within the HOCR).

The survey found that the most common technology-related activity amongst young people was illegal downloading. In the 2004 OCJS around one in four (26%) 10- to

[21] Note: not all participants in this study were necessarily victims of online fraud – the offence categories could include 'offline' behaviours, such as supplying false fronts for cash machines, or phishing via SMS or phone.

25-year-old internet users reported that they had illegally downloaded software, music or files in the 12 months prior to the survey (Wilson *et al.*, 2006).

Other forms of cyber-enabled offending were rare. The number of young people who reported obtaining someone else's card details over the internet was very low (0.1% of all 12- to 25-year-olds), and the same proportion reported buying goods or services over the internet using someone else's card details without the card owner's permission (0.1% of 12- to 25-year-olds).

Full details relating to other forms of offending captured in the survey are outlined in Chapter 1: Cyber-dependent crimes.

Methods

The methods used in cyber-enabled fraud and data theft to obtain or use compromised data may incorporate a number of technical and social engineering techniques, including the use of malware and hacking. These are outlined in Chapter 1: Cyber-dependent crimes. The products from cyber-dependent crimes (e.g. bank account information or other personal data), may subsequently be sold via online forums or marketplaces to be used for fraudulent purposes.

Insider vs. outsider attacks against business and industry

Security breaches may stem from clear outsider attacks, i.e. an external hack, which relies on the technical skills of the offender and vulnerabilities in systems or networks. It is also possible that members of staff may inadvertently assist perpetrators with this, for example, downloading an attachment from a suspicious file.

'Insider threats' from members of staff may be malicious and targeted activity, for example, someone seeking revenge if they know they are about to be fired. However, they may also be accidental or generally negligent, for example, emailing data to the incorrect person, or losing a memory stick (and recorded as data loss rather than theft).

Case-study 2

Insider fraud: A case-study

A debt-ridden accountant who stole more than £24,000 from her pension fund employer was warned that she was 'lucky' to avoid jail. [The cyber fraudster] siphoned off the cash over a two-year period to buy groceries and pay her mortgage after substituting her own bank details for those of suppliers.

[She] stole around £1,000 a month until a trainee became suspicious about outgoing payments that were recorded on her own computer login, but that she could not remember processing.

Court News UK, 2012

Insider-threats are a prominent issue reported in business surveys. However, the limited evidence available is mixed regarding whether they are a bigger problem than outsider attacks. From a survey of 1,007 businesses (BERR, 2008) over a half (57%) of the most serious incidents had an internal cause, whereas 38 per cent had an external cause. This represented a shift from 2006 when more than two-thirds (68%) were regarded as external. However, the majority (86%) of recent incidents reported

by businesses in the Commercial Victimisation Survey (2013b) were thought to be have been undertaken by someone targeting computer systems from outside of the organisation, rather than by someone physically accessing computers at the premises (2%). The remaining 12 per cent did not know whether systems had been targeted internally or externally (although it was not possible to verify the accuracy of these reports). However, this difference may reflect the different scope of the two surveys, making direct comparisons problematic, rather than being a 'true' shift in the nature of the threat.

Potential security concerns have also been raised in recent research regarding the outsourcing of business processes to external providers and in relation to new forms of data storage such as cloud computing (PwC, 2012). However, there is a lack of robust research available to provide evidence of the precise extent of the risk.

References

Action Fraud (2012) Unpublished data. London: National Fraud Authority.

Action Fraud (2013). *The Devil's in Your Details*. Retrieved June 2013. Available at: <http://www.actionfraud.police.uk/thedevilsinyourdetails>.

Anderson, R., Barton, C., Bohme, R., Clayton, R., van Eeten, M. J. and Levi, M. (2012) *Measuring the cost of cybercrime*. Retrieved September 2013. Available as: <http://weis2012.econinfosec.org/papers/Anderson_WEIS2012.pdf>.

Allen, J., Forrest, S., Levi, M., Roy, H., and Sutton, M. (2005) *Fraud and Technology Crimes: Findings from the 2002/3 British Crime Survey and 2003 Offending, Crime and Justice Survey.* Online Report 34/05. London: Home Office.

APWG. (2012) *Phishing Activity Trends Report (2nd Quarter 2012).* Retrieved September 2013. Available at: <http://docs.apwg.org/reports/apwg_trends_report_q2_2012.pdf>.

APWG. (2013) *Phishing Activity Trends Report (4th Quarter).* Retrieved September 2013. Available at: <http://docs.apwg.org/reports/apwg_trends_report_q4_2012.pdf>.

BERR (2008) *Information Security Breaches Survey.* London: Department for Business, Innovation and Skills. Retrieved from BIS, September 2013. Available at: <http://www.bis.gov.uk/files/file45714.pdf>.

BRC. (2012) *Counting the cost of E-Crime.* Retrieved September 2013. Available at: <http://www.martinfrost.ws/htmlfiles/aug2012/counting-cost-ecrime.pdf>.

Computer Misuse Act 1990.

Court News UK (2012) 'Bailey: Accountant escapes jail over £24k thefts', *Court News UK*, September 17 2012. Retrieved September 2013. Available at: <http://www.courtnewsuk.co.uk/online_archive/?name=A+debt-ridden+accountant+&place=&courts=0>.

Detica (2011) *The Cost of Cybercrime.* London: Cabinet Office. Retrieved September 2013. Available at: <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60943/the-cost-of-cyber-crime-full-report.pdf>

Dutton, W. H. and Blank, G. (2013). *Cultures of the Internet: The Internet in Britain.* Oxford: Oxford Internet Institute, University of Oxford. Retrieved September 2013. Available at: <http://oxis.oii.ox.ac.uk/sites/oxis.oii.ox.ac.uk/files/content/files/publications/OxIS_2013.pdf>.

Eurobarometer (2012) *Cyber Security: UK.* European Commission.

Eurostat. (2010) *Internet Usage in 2010 - Households and Individuals.* Retrieved September 2013. Available at: <http://epp.eurostat.ec.europa.eu/cache/ITY_OFFPUB/KS-QA-10-050/EN/KS-QA-10-050-EN.PDF>.

Federal Bureau of Investigation. (2009, January 4) *Spear Phishers*. Retrieved June 2013. Available at: <http://www.fbi.gov/news/stories/2009/april/spearphishing_040109/>.

Federal Trade Commission. (2006) *Identity Theft Survey Report.* Retrieved September 2013. Available at: <http://www.ftc.gov/os/2007/11/SynovateFinalReportIDTheft2006.pdf>.

Financial Fraud Action (2012) *Fraud the Facts.* Retrieved from UK Cards Association, September 2013. Available at: <http://www.theukcardsassociation.org.uk/wm_documents/Fraud_The_Facts_2012.pdf>.

Financial Fraud Action (2013) *Fraud the Facts 2013.* Retrieved September 2013. Available at: <http://www.financialfraudaction.org.uk/publications/files/assets/basic-html/page1.html>.

Finch, E. (2003) 'What a tangled web we weave: identity theft and the internet', In *Dot Cons: Crime Deviance and Identity on the Internet,* Jewkes, Y., pp. 86-104. Culhompton: Willan Publishing.

Fletcher, N. (2007) 'Challenges for regulating financial fraud in cyberspace', *Journal of Financial Crime* , 14(20), pp 190-207.

Florencio, D., and Herley, C. (2011) 'Sex, lies and cyber crime surveys', *Economics of Information Security and Privacy III*, pp 35-53.

Get Safe Online. (2012) *Annual Survey 2011.* Retrieved July 2013. Available at: <https://www.getsafeonline.org/about-us/>.

Home Office (2011) *The National Crime Recording Standard (NCRS): What you need to know.* London: Home Office. Retrieved August 2013. Available at: <www.gov.uk: https://www.gov.uk/government/publications/the-national-crime-recording-standard-ncrs-what-you-need-to-know>.

Home Office (2012) *Counting Rules for Recorded Crime*. London: Home Office. Retrieved September 2013. Available at: <http://homeoffice.gov.uk/science-research/research-statistics/crime/counting-rules/>.

Home Office (2013a) *Crime against businesses: Headline findings from the 2012 Commercial Victimisation Survey.* Retrieved September 2013. Available at: <http://www.homeoffice.gov.uk/publications/science-research-statistics/research-statistics/crime-research/crime-business-prem-2012/crime-business-prem-2012-pdf?view=Binary >.

Home Office (2013b) *Commercial Victimisation Survey* [computer file]. UK: ONS. Retrieved September 2013. Available at: <https://www.gov.uk/government/publications/crime-against-businesses-detailed-findings-from-the-2012-commercial-victimisation-survey>.

ICO. (2012, September 19) Personal Communication.

Ipsos MORI (2013) *A survey of public attitudes to Computer Security.* Home Office Research Report 75 (Annex B). London: Home Office.

Kerr, J., Owen, R., McNaughton Nicholls, C., and Button, M. (2013) *Research on Sentencing Online Fraud Offences.* Retrieved September 2013. Available at: <http://sentencingcouncil.judiciary.gov.uk/docs/Research_on_sentencing_online_fraud_offences.pdf>.

McGuire, M. (2007) *Hypercrime: The new geometry of harm.* Routledge.

McGuire, M. (2012) *Organised Crime in the Digital Age.* Detica/BAE.

McQuade, S. (2006) *Understanding and Managing Cybercrime.* Boston: Allyn & Bacon.

Ministry of Justice. (2013) *Criminal Justice Statistics - Quarterly Update to March 2013, England and Wales.* Retrieved September 2013. Available at: <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/231011/criminal-justice-stats-march-2013.pdf>.

National Fraud Authority (2011) *A Quantitative Segementation of the UK Population: Helping Determine How and When Citizens become Victims of Fraud.* Retrieved September 2013. Available at: <http://www.homeoffice.gov.uk/publications/agencies-public-bodies/nfa/national-fraud-segmentation>.

National Fraud Authority (2013) *Annual Fraud Indicator.* Retrieved September 2013 Available at: <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/206552/nfa-annual-fraud-indicator-2013.pdf>.

Ofcom (2012) *Communications Market Report.* London: Ofcom. Retrieved from Ofcom, September 2013. Available at: <http://stakeholders.ofcom.org.uk/binaries/research/cmr/cmr12/CMR_UK_2012.pdf>.

Ofcom (2013) *Adults media use and attitutdes report.* London: Ofcom. Retrieved September 2013. Available at: <http://stakeholders.ofcom.org.uk/binaries/research/media-literacy/adult-media-lit-13/2013_Adult_ML_Tracker.pdf>.

OFT (2006) *Research on impact of mass marketed scams: A summary of research into the impact of scams on UK consumers.* London: Office of Fair Trading.

OFT (2009) *Findings from consumer surveys on internet shopping: A comparison of pre- and post-study consumer research.* London: Office of Fair Trading. Retrieved September 2013. Available at: <http://www.oft.gov.uk/shared_oft/reports/Evaluating-OFTs-work/oft1079.pdf>.

ONS (2010) *Internet Access 2010: Households and individuals.* UK: Office for National Statistics. Retrieved September 2013. Available at: <http://www.google.co.uk/url?sa=t&rct=j&q=&esrc=s&frm=1&source=web&cd=2&ved=0CDgQFjAB&url=http%3A%2F%2Fwww.ons.gov.uk%2Fons%2Frel%2Frdit2%2Finternet-access---households-and-individuals%2F2010%2Fstb-internet-access---households-and-individuals--2010.pdf&ei=>.

ONS (2012) *Crime Survey for England and Wales, 2011/12* [computer file]. UK: ONS. Retrieved September 2013. Available at: < http://www.ons.gov.uk/ons/rel/crime-stats/crime-statistics/focus-on-property-crime--2011-12/index.html>.

ONS (2013) *Crime in England and Wales, Year Ending March 2013.* Retrieved September 2013. Available at <http://www.ons.gov.uk/ons/dcp171778_318761.pdf>.

Poneman Institute (2012) *Cost of Data Breach Study: United Kingdom.* Retrieved August 2013. Available at: <http://www.ponemon.org/local/upload/file/2011_UK_CODB_FINAL_5.pdf>.

PwC (2012) *2012 Information Security Breaches Survey.* Retrieved September 2013. Available at <http://www.pwc.co.uk/en_UK/uk/assets/pdf/olpapp/uk-information-security-breaches-survey-technical-report.pdf>.

PwC (2013) *2013 Information Security Breaches Survey.* Retrieved September 2013. Available at <http://www.pwc.co.uk/assets/pdf/cyber-security-2013-technical-report.pdf>.

RSA (2012) *Online Fraud Report.* Retrieved September 2013. Available at: <www.rsa.com: http://www.rsa.com/phishing_reports.aspx>

Smith, R. (2006) *Identification systems: A risk assessment framework.* Australian Insitute of Criminology, Australian Government. Canberra: Trends and Issues in Crime and Criminal Justice.

The Scottish Government (2011) 2010/11 Scottish Crime and Justice Survey: Main Findings. Edinburgh: The Scottish Government. Retrieved September 2013. Available at: **<**http://www.scotland.gov.uk/Resource/Doc/361684/0122316.pdf>.

Whitty, M. and Buchanan, T. (2012) 'The online romance scam: A serious cybercrime', *CyberPsychology, Behavior, and Social Networking*, 15 (3), pp 181–183.

Wilson, D., Patterson, A., Powell, G., and Hembury, R. (2006) *Fraud and technology crimes: Findings from the 2003/04 British Crime Survey, the 2004 Offending, Crime and Justice Survey and administrative sources.* Retrieved September 2013. Available at: <http://webarchive.nationalarchives.gov.uk/20110220105210/rds.homeoffice.gov.uk/rds/pdfs06/rdsolr0906.pdf>.

ISBN: 978-1-78246-245-3