Home Office

Cyber crime: a review of the evidence

Samantha Dowling
Cyber Crime Research
Home Office Science

Dec 2013

Purpose of the evidence review

- Set in context of the National Cyber Security Strategy (2011) and the Serious and Organised Crime Strategy (2013).

- Improve our understanding of the scale and nature of cyber crime - what do we know, how reliable is it, where are the gaps?

- Focus on:
  - Published evidence, from academic, government and industry sources.
  - UK-specific evidence, dated from 2000.
  - Cyber-dependent and two forms of cyber-enabled crime (fraud and theft; sexual offending against children).
  - Evidence regarding scale, cost, methods, victims, offenders.

Full publication available at:

https://www.gov.uk/government/publications/cyber-crime-a-review-of-the-evidence

Cyber crimes divide into two main categories: those that are cyber-dependent and those that are cyber-enabled

Cyber crime is an umbrella term, which can be divided into two main types :

- **Cyber-dependent crimes**, which can only be committed by using a computer, computer network or other form of Information Communication Technology (ICT). They are primarily acts directed against computers or network resources and are typically offences under the Computer Misuse Act (CMA).
- **Cyber-enabled crimes –** 'traditional' crimes which are increased in their scale or reach by use of computers, computer networks or other ICT, although they can be still be committed without the use of ICT.

- Crimes that relate to **online abuse** (e.g. harassment, stalking, trolling etc) are not covered in depth by the cyber evidence review.

Cyber-dependent

- Spread of viruses and other malware
- Hacking
- Distributed Denial of Service attacks (DDoS) *i.e. the flooding of internet servers with multiple requests causing them to crash.*

Cyber-enabled

- Fraud
- Data theft
- Grooming
- Distributing child porn
- Sale of illegal drugs

Presentation outline

1) Cyber-dependent crimes
   - Victimisation surveys
   - Action Fraud data
   - Ministry of Justice data
   - Anti-virus company data

2) Cyber-enabled fraud
   - Victimisation surveys
   - Action Fraud data
   - Banking sector data

3) Under-reporting

4) Summarising the cyber landscape

5) Challenges and data limitations

6) Improving the evidence base

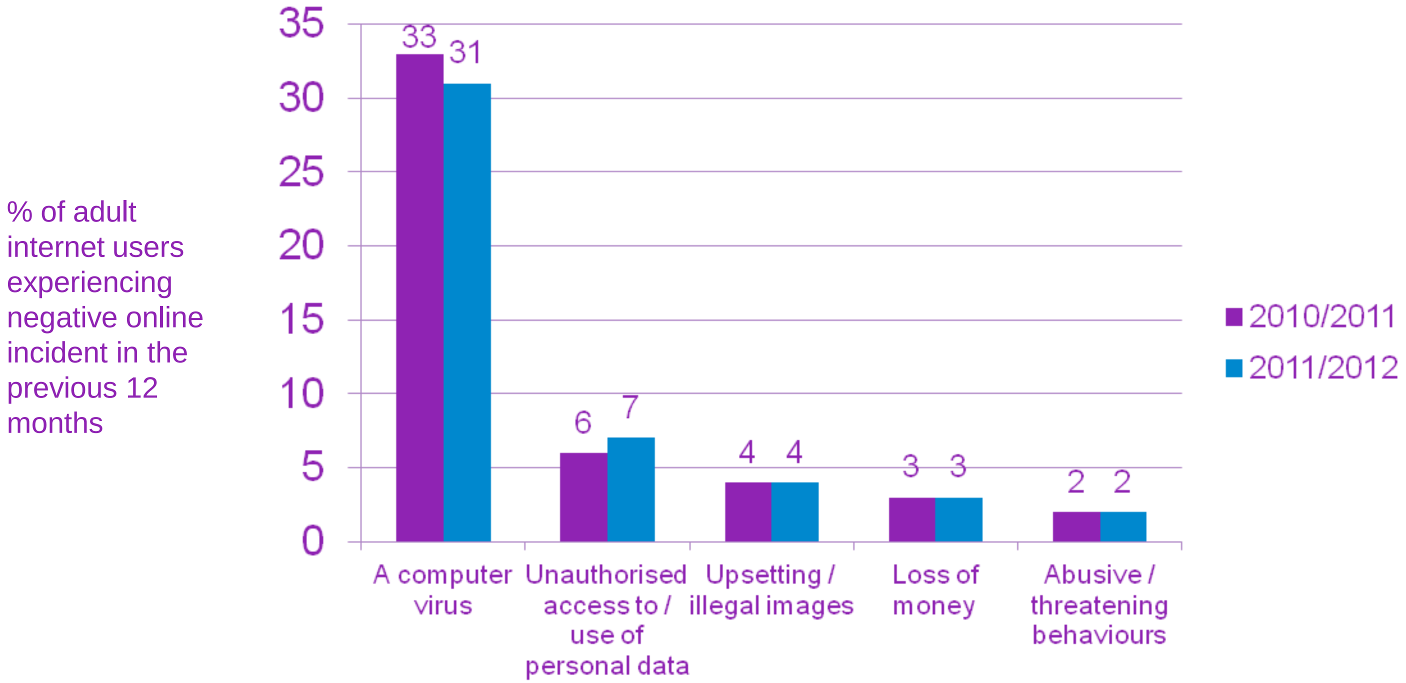
1) Cyber-dependent crime

Public experiences of ‘negative online incidents’ - the Crime Survey for England and Wales (CSEW)

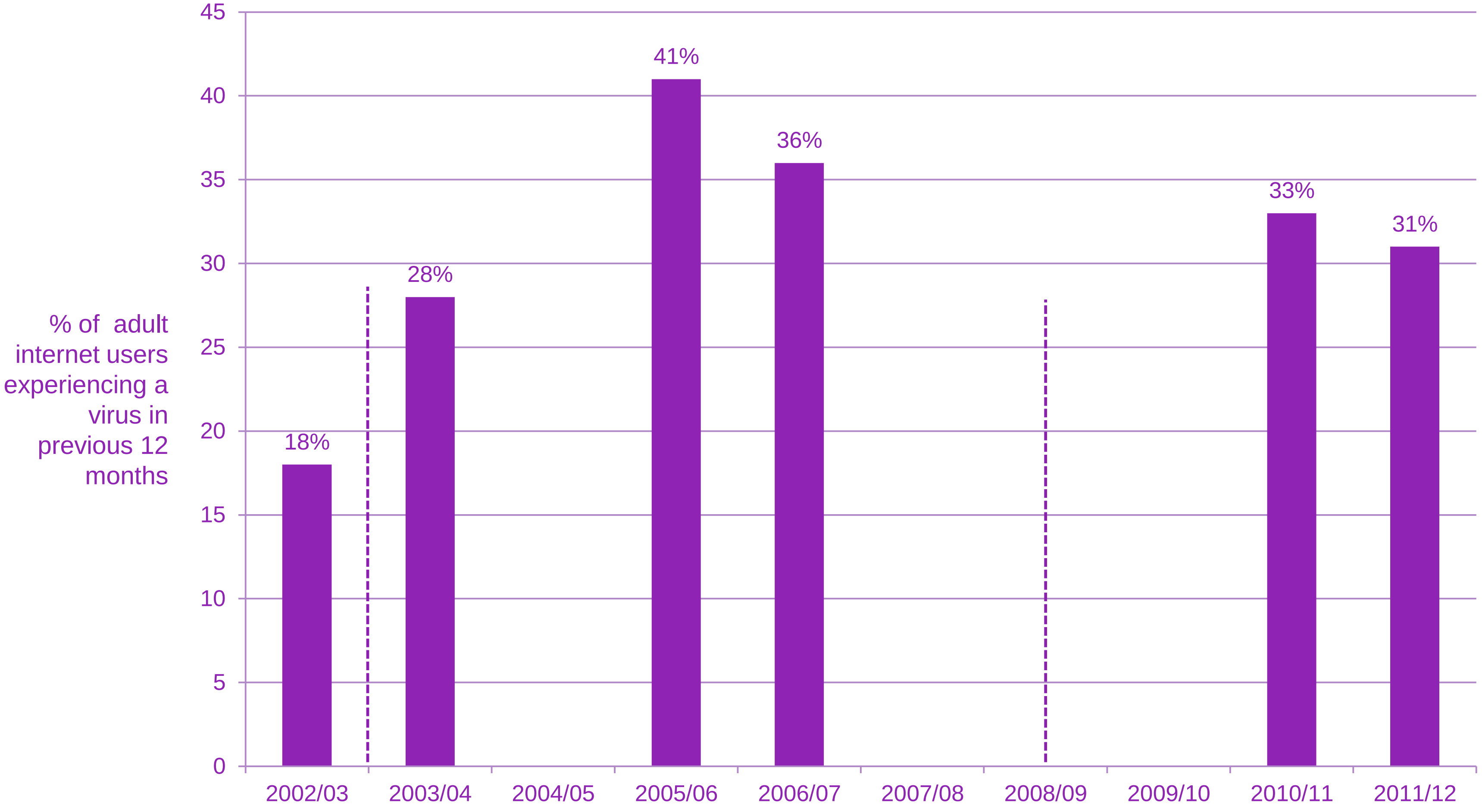
- In 2011/12 over one-third (37%) of adult internet users reported experiencing one or more negative online incidents in the past 12 months. A statistically significant decrease from 39% in 2010/11.

- However, CSEW data doesn’t relate to criminal activity per se. These experiences are likely to be below the threshold of a recorded crime under Home Office Counting Rules.

Negative experiences in the last year among internet users aged 16 and over, CSEW, 2010/11 and 2011/12



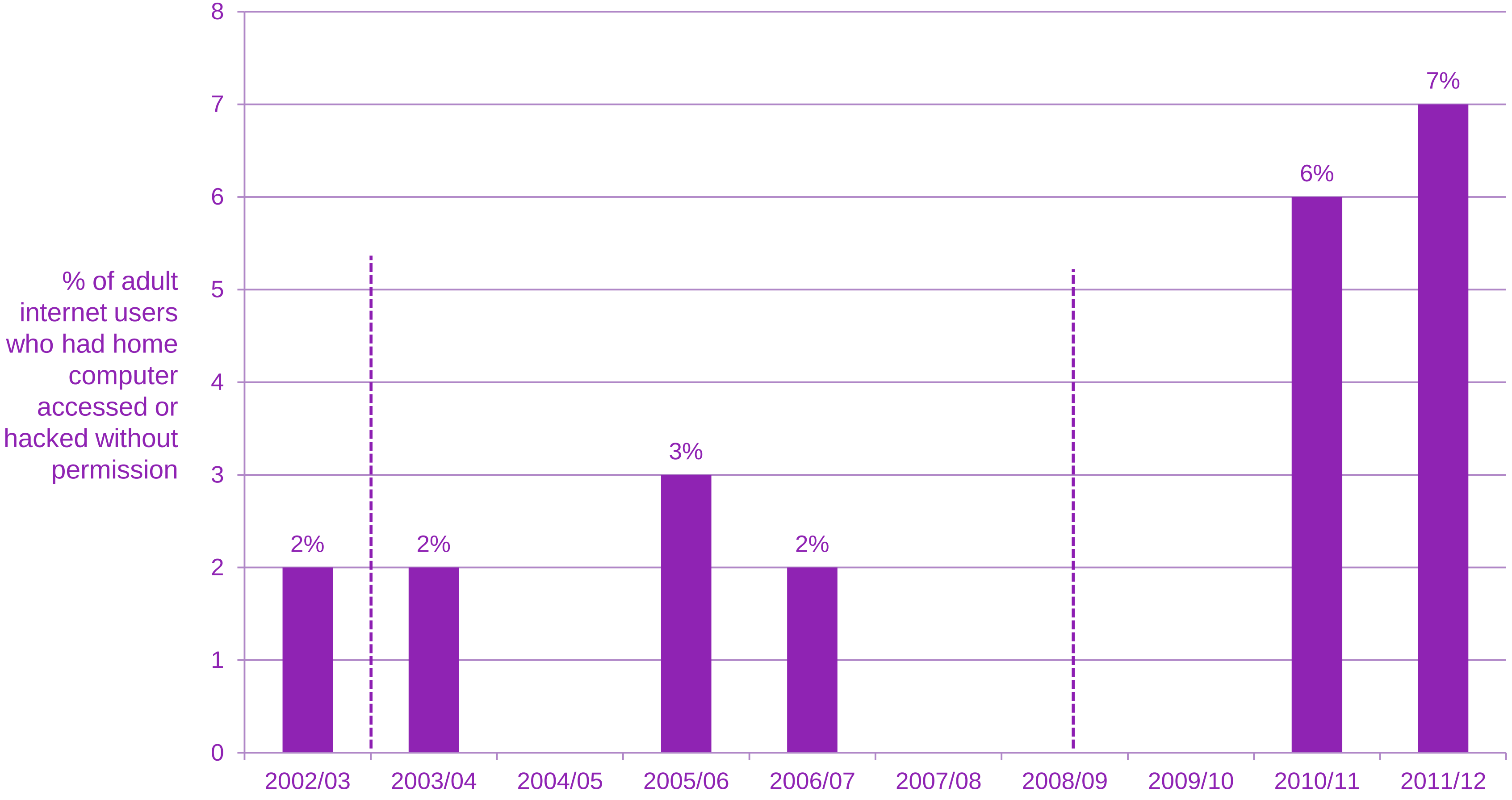
CSEW data suggests the percentage of adult internet users experiencing computer viruses appears to be falling…



Source: CSEW. Changes (year-on-year) are statistically significant at the 0.05 level.

Dotted lines relate to changes in the wording of the question. Due to these changes, figures are not directly comparable.
2002/03: Has your HOME computer been affected by a computer virus?
2003/04-2006/07: Has your home computer been damaged by a virus, [or] been infected by a virus but not actually damaged?
2010/11-2011/12: Have you personally experienced a computer virus?

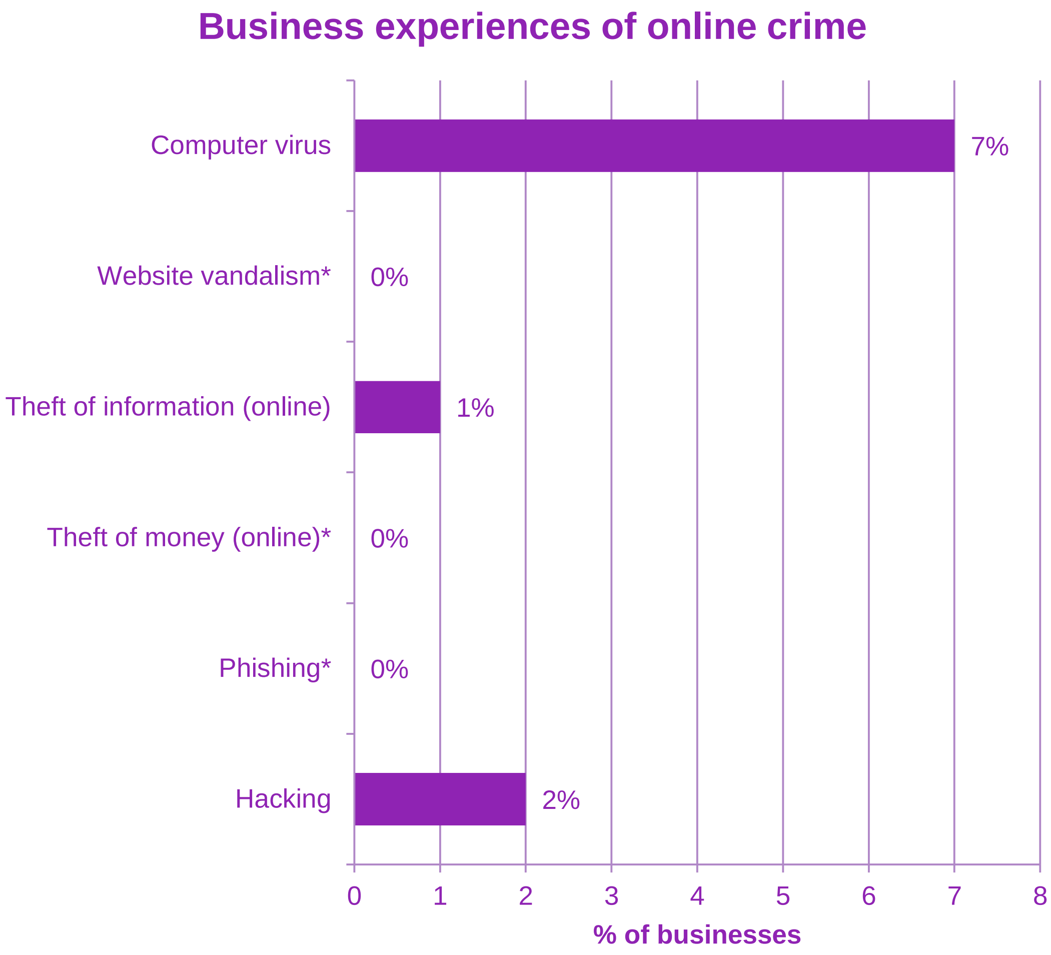
…whilst the proportion of individuals who have had their personal computers accessed or hacked without their permission appears to have increased since the 2000s.



Source: CSEW. There were statistically significant changes between 2003/04-2005/06, and 2006/07-2010/11.

Dotted lines relate to changes in the wording of the question. Due to these changes, figures are not directly comparable.
2002/03-2006/07: In the last 12 months, has anyone accessed or hacked into the files on your home computer without your permission?
2010/11-2011/12: Have you personally experienced unauthorised access to/use of personal data (e.g. email account, bank account?

Businesses can also be victims of online ‘crime’. Computer viruses are the most common experience amongst businesses, according to the Commercial Victimisation Survey.



* Less than 0.5 per cent of businesses experience this kind of online ‘crime’.

Source: Commercial Victimisation Survey, 2012

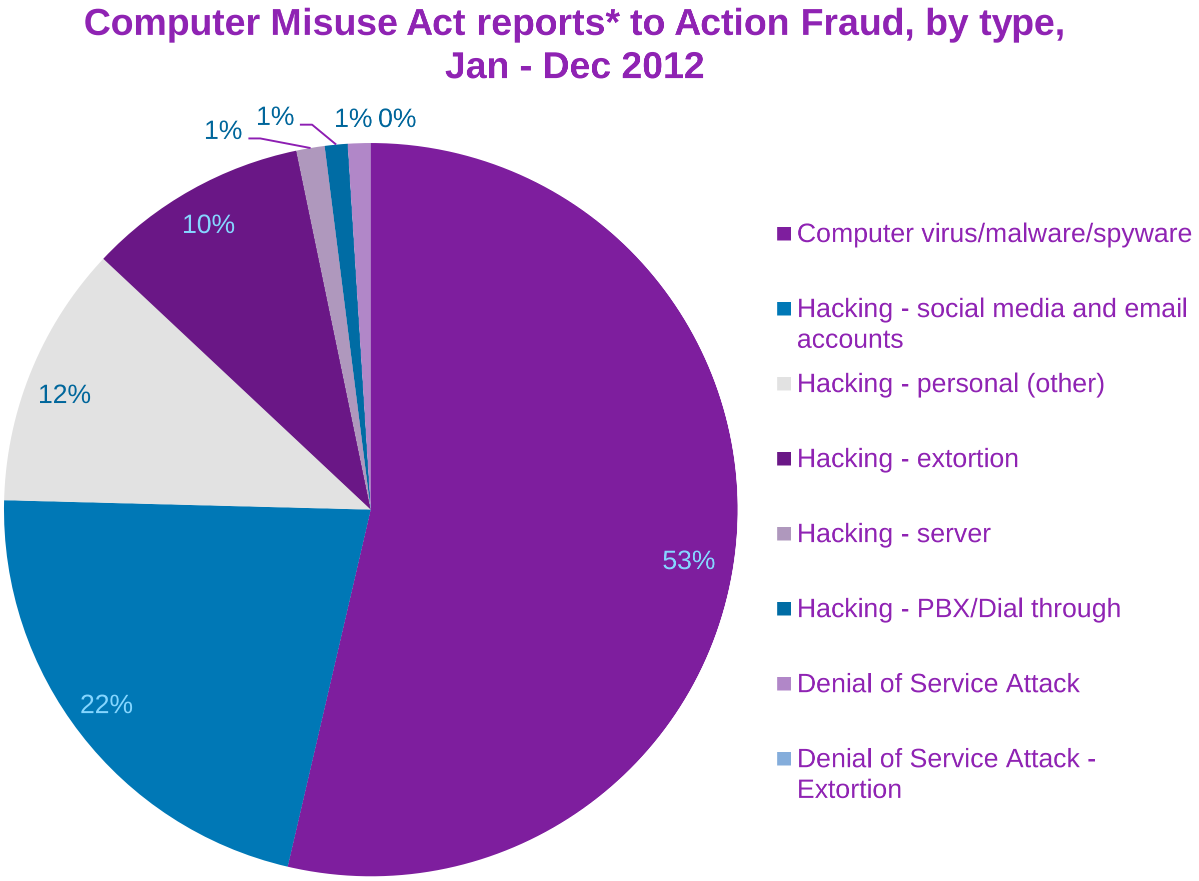
8% of business premises in England and Wales, across the four sectors covered by the CVS, experienced at least one type of online crime in the previous 12 months, which equated to 180,000 incidents (CVS 2012). Three-quarters of these incidents were computer viruses.

However, as with the CSEW, not all the incidents reported in the CVS would be classed as ‘crimes’ in accordance with the HOCR.

The CVS is a survey of business premises, and excludes head offices and other business sectors (including financial services). So some online crimes may not be picked up by the CVS. The results of the CVS are representative of crimes against the four sectors surveyed, but not against business as a whole.

Figures are based on four sectors: accommodation and food; transportation and storage; wholesale and retail; and manufacturing.

Looking at Action Fraud reports, of the over 7,000 incidents and crimes which related to offences under the Computer Misuse Act in 2012, over half were malware, virus and spyware reports



**‘Hacking – social media’ refers to any unauthorised access to an individual’s social media, such as Facebook, and individual email accounts.

‘Hacking – personal’ refers to any incident where unauthorised access is gained to personal computing equipment, including internet-connected devices such as games consoles and smart phones.

* Figures include reports of crimes and ‘information’ reports. Action Fraud is a national fraud reporting centre that records incidents of fraud directly from the public as well as from the police (five forces began reporting in Jan 12, which rose to 24 forces in Dec 12). Figures include reports of crimes and ‘information’ reports.

MoJ data shows how few people are sentenced under the CMA.

– During 2007-2012 there were 101 people initially proceeded against and 88 people sentenced with a primary offence under the CMA (Ministry of Justice, 2011).

– This reflects that most individuals are being proceeded against for cyber offences under other Acts such as the Fraud Act.

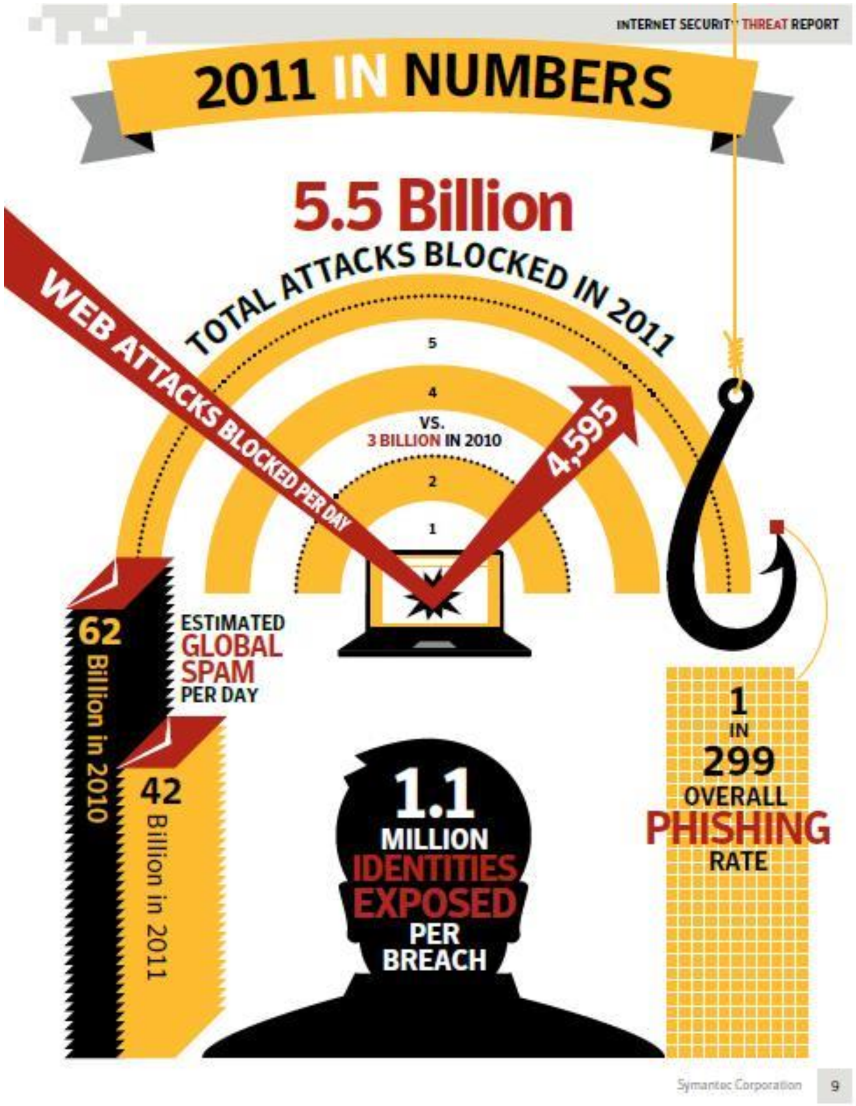
What can industry sources tell us? Symantec reported 5.5 billion ‘attacks blocked’ in 2011.

But AV reports are hard to compare:

- Different anti-virus companies use different units of measurement.
- Different companies have different geographical coverage and customer bases.
- General lack of transparency in the methodologies used to produce estimates of infections and attacks.
- British Society of Computing recommends ‘caution’ with use of industry figures (2012).

– On the other hand, AV reports are helpful in informing the nature of various threats and tend to concur on broad trends.

– *“The reality is the problem isn’t as big as we think – but we don’t really have a good way of quantifying it”*…we need to put the *“science back into computer science” .* (John Viega, VP U.S Perimeter E-Security Company).



2) Cyber-enabled fraud

There are various forms of online fraud and scams

- **Fraudulent sales through online auction sites (e.g. E-bay) or bogus retail websites.** Once paid for, goods or services are not delivered or buyers unknowingly purchase counterfeit products (e.g. online ticketing fraud).

- **Consumer scams** (e.g. advance fee frauds such as 419 fraud, inheritance or lottery frauds). Individuals are persuaded to part with money upfront, e.g. to help someone invest in a business, on the promise that a larger sum of money will be returned to them at a later date.

- **‘Online romance’ frauds.** Individuals may be persuaded to part with personal information or money following a lengthy online ‘relationship’ via dating sites.

- **E-commerce frauds.** The fraudulent use of plastic cards to make online retail purchases.

- **Online banking fraud.** Where criminals fraudulently gain access to online bank accounts.

Only a small proportion of internet users appear to have fallen victim to cyber-enabled frauds, but many 'victims' would be refunded by a bank.

Survey	Type of fraud/scam measured	Key findings
CSEW 2011/12	Receipt of potential fraud related communications (e-mail, text, letter and phone call)	56% received stated receiving one or more potentially fraud-related communications. (no. falling victim is unknown).
Ipsos-Mori (2013)	Experiencing financial loss from credit/debit card misuse online.	5% of internet users reported this in the 12 months prior to March 2012
OfT (2006)	Online and Offline Mass marking scams	2% fell victim
Whitty and Buchanan (2012)	Financial loss from internet dating scams	Less than 1% lost money

However the proportions of internet users being attacked by phishing emails appears to be increasing...

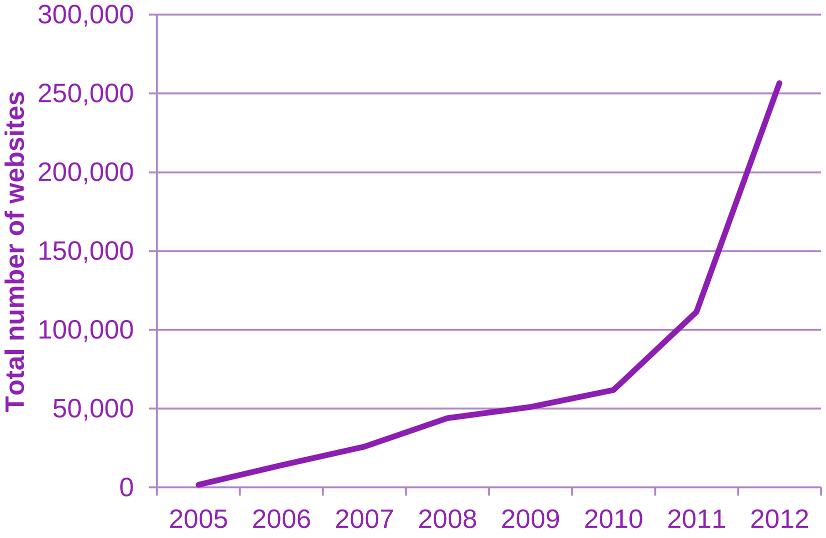
- Some spam emails are deliberate attempts to ‘fish’ for personal information to facilitate fraud. These are commonly referred to as ‘phishing’ emails.

- Phishing attempts appear to be increasing. Twenty two per cent of UK internet users experienced phishing attempts in 2011, up from twelve per cent 2005 (Oxford Internet Institute, 2011).

- Despite the increase in the proportion of users who report receiving phishing emails, the proportion of internet users who report losses is small (around 3 per cent in 2010, according to the ONS).

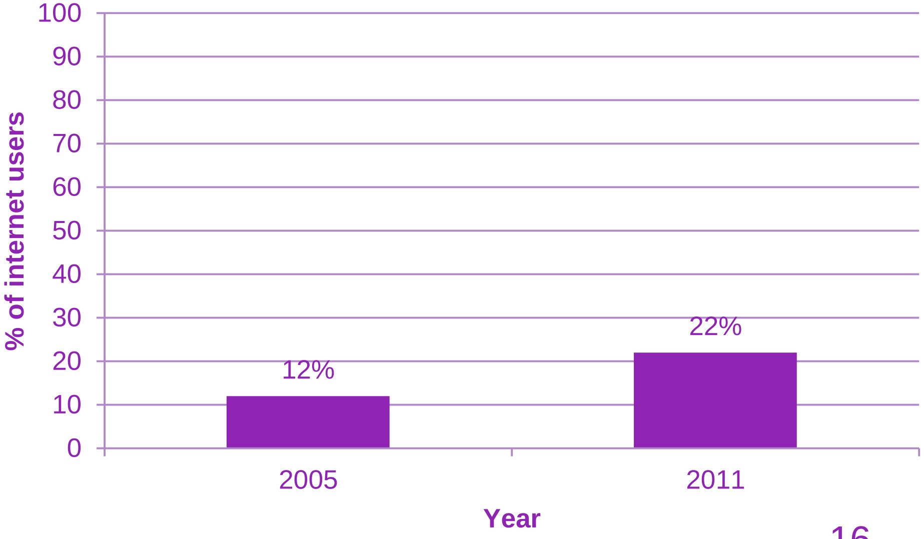
- There has been a large increase in the total number of phishing websites targeted against UK banks and building societies, i.e. fake websites designed to look like those of genuine organisations, in order to trick people into entering their personal information.

Total number of phishing websites targeted against UK banks and building societies



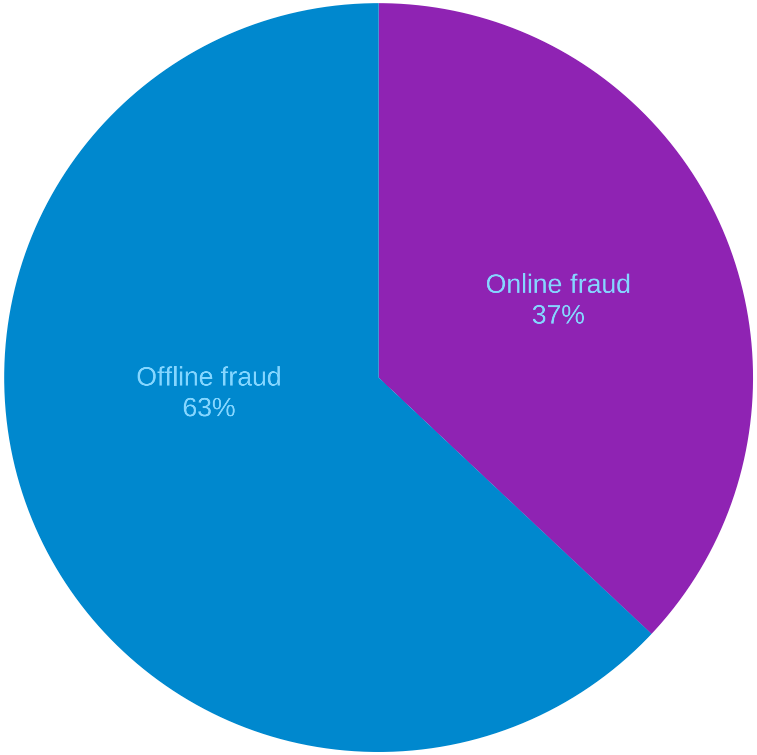
Source: Financial Fraud Action

Percentage of current internet users who were asked to provide their bank details (phishing)



Source: Oxford Internet Institute, 2011

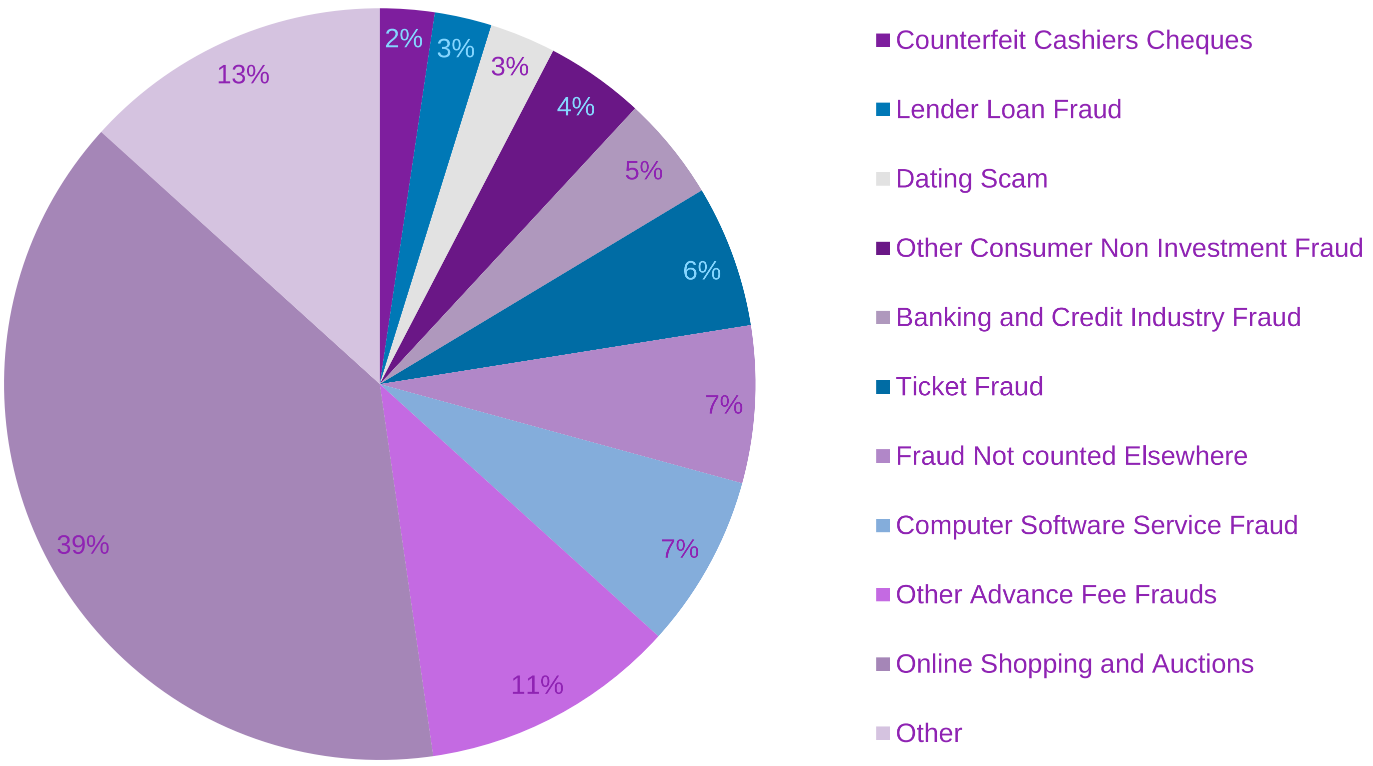
Nearly four in ten of the 130,000 frauds reported to Action Fraud in 2012 took place online*



* Figures include reports of crimes and ‘information’ reports. These data exclude 7,000 Computer Misuse Act Offences (see slide 8). Action Fraud is a national fraud reporting centre that records incidents of fraud directly from the public as well as from the police (five forces began reporting in Jan 12, which rose to 35 forces in Dec 12). Figures include reports of crimes and ‘information’ reports.

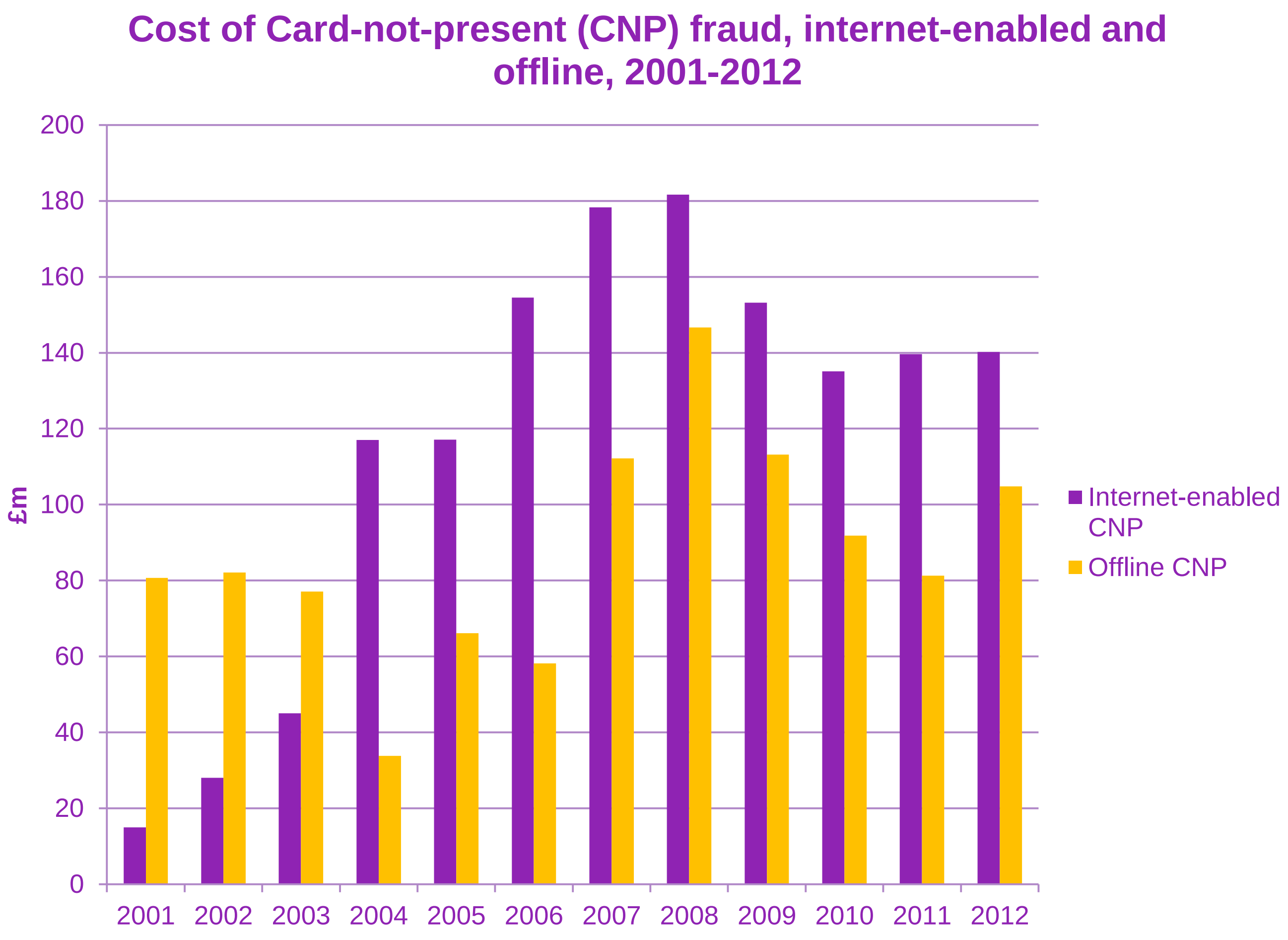
Of the 48,000 online frauds reported to Action Fraud in 2012, the largest category was frauds involving online shopping and auctions (one third of the total)

Online frauds reported* to Action Fraud by type, Jan-Dec 2012



* Figures include reports of crimes and ‘information’ reports. Action Fraud is a national fraud reporting centre that records incidents of fraud directly from the public as well as from the police (five forces began reporting in Jan 12, which rose to 35 forces in Dec 12). Figures include reports of crimes and ‘information’ reports.

Losses to the banking system as a result of online shopping/e-commerce fraud on plastic cards increased rapidly in the early 2000s. But they have fallen since 2008, in part at least due to improved security features



Note: Figures from Financial Fraud Action represent losses to the banking/payments sector, not the retail sector

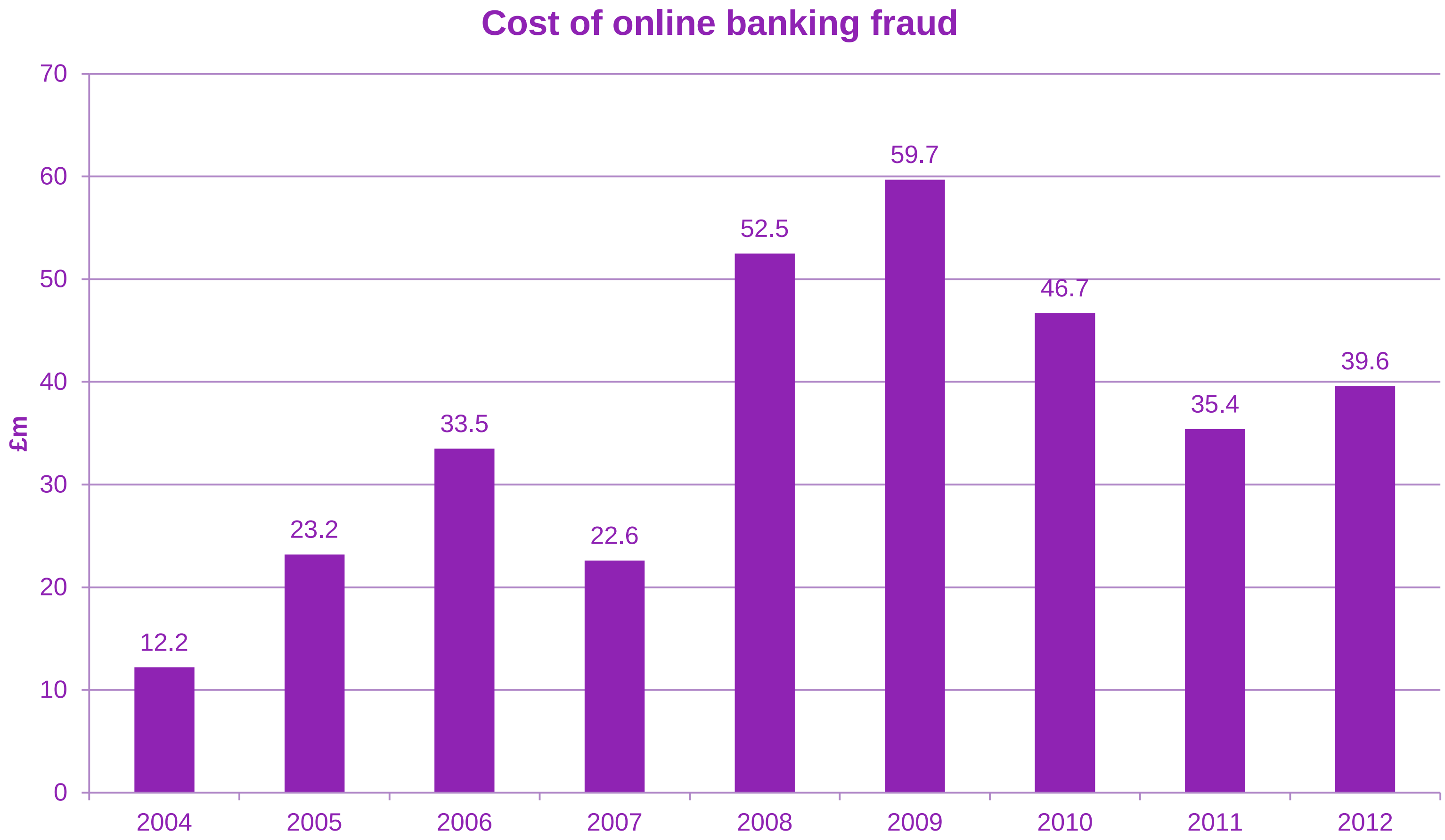
Card-not-present (‘CNP’) fraud involves transactions conducted remotely (i.e. via the internet, over the phone or mail-order), where neither cardholder nor card are present.

The chart shows the value of internet-enabled card-not-present fraud and offline (e.g. telephone) card-not-present fraud. Offline CNP fraud declined in the early 2000s with the growth of internet shopping (and related fraud), but has risen since.

Internet-enabled CNP declined post 2008 partly due to the introduction of security measures such as American Express SafeKey; Mastercard SecureCode and Verified by Visa.

Source: Financial Fraud Action, 2012

Losses from online banking fraud have declined since 2009

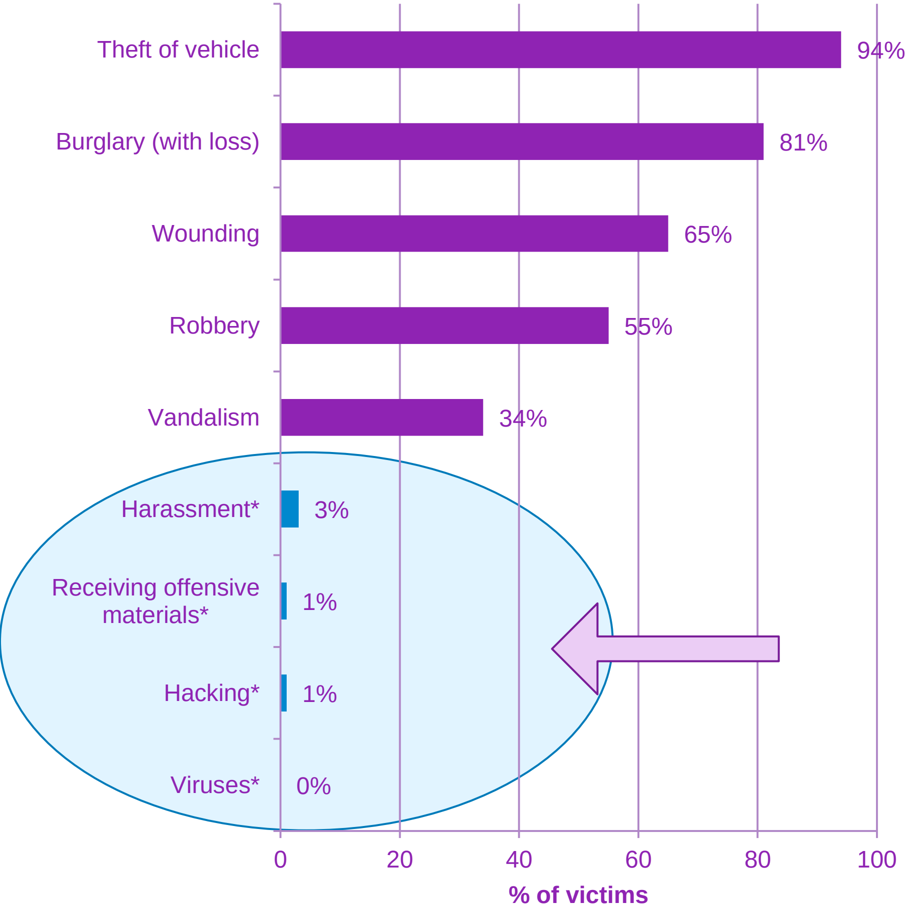


Source: Financial Fraud Action, 2012

3) Under-reporting

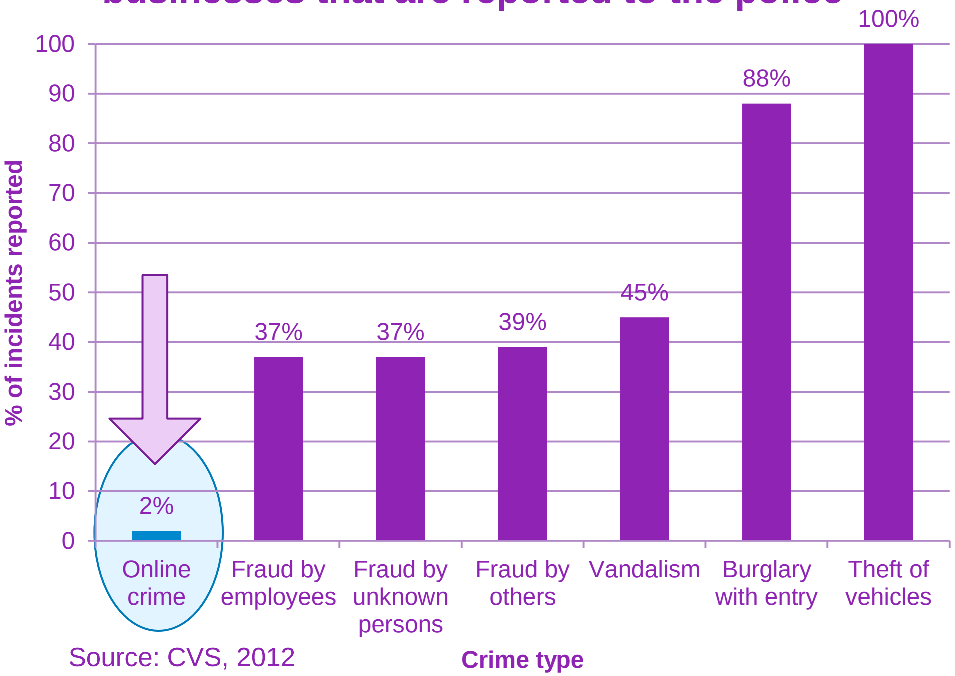
Online incidents and crimes are reported to the police (or Action Fraud) far less often than offline crime. Only one per cent of adult internet users experiencing hacking reports this to the police

Rates of reporting crime and negative online incidents to the police, by the general public



Source: CSEW, 2006/07. *relates to all adult internet users

Proportion of incidents experienced by businesses that are reported to the police

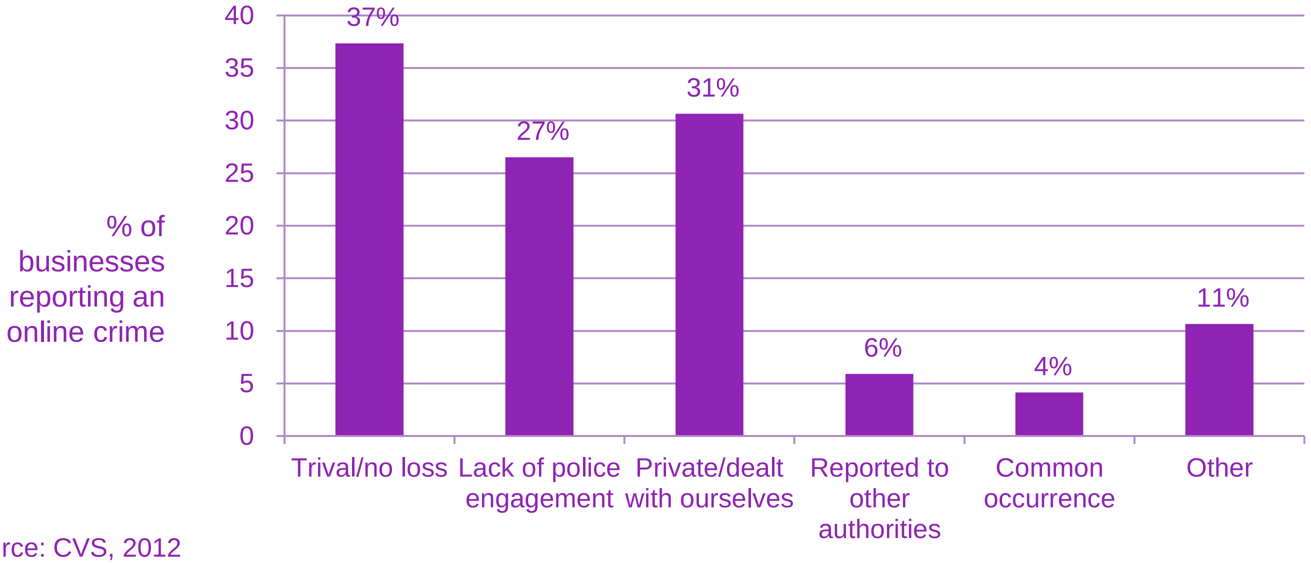


Source: CVS, 2012

Why is online crime so under-reported to the police?

- Victims do not realise that the incident is a crime or consider it too trivial to report;
- Victims do not realise that they have been targeted;
- Victims do not consider themselves to be victims (e.g. if they have been reimbursed by a financial institution, and therefore have suffered no loss, they may not perceive a crime to have been committed);
- Unlike much acquisitive crime, there is often no need for a crime report to bring about reimbursement e.g. banks often do not require customers to report incidents to the police;
- Sometimes incidents/crimes are reported to other bodies, such as Internet Service Providers.

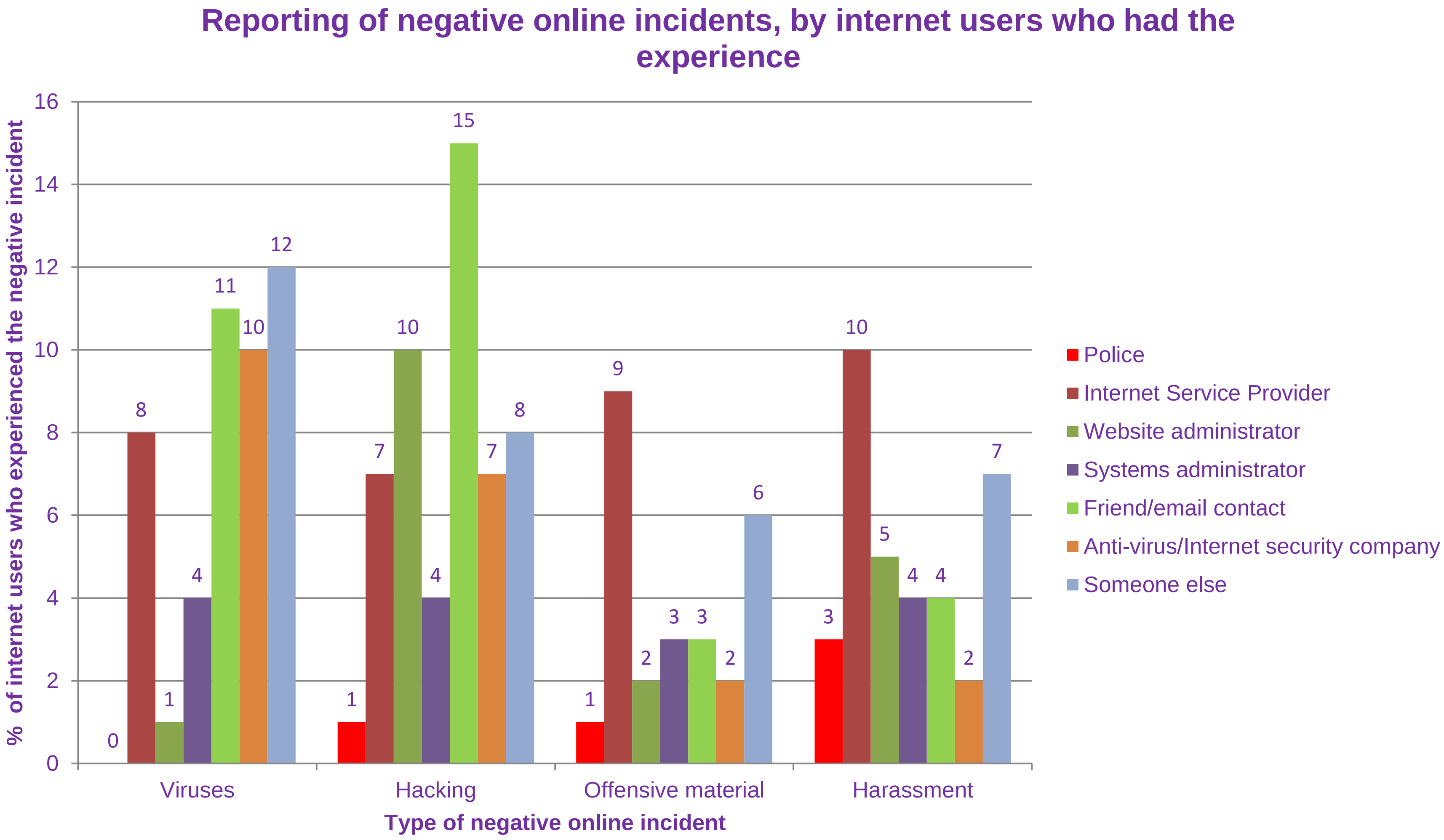
Business victims – reasons for not reporting to the police



Business victims of online crime were most likely not to report to the police because the incident was trivial / no loss (37%) or described as ‘private, dealt with ourselves’ (31%).

Source: CVS, 2012

Although reporting of negative online incidents to the police is low, individuals do report to others, most commonly Internet Service Providers



Source: CSEW, 2006/07

4) How could we summarise the cyber landscape?

- Given the range of crimes involved we cannot make statements about ‘cyber crime’ as a whole - we can say something about <u>different types </u>of cyber crimes.
- Knowledge regarding some types of cyber crime is more developed than others. We draw on a range of sources to build a patchwork of evidence.
- Yet the quality of available data is variable. Good quality evidence is limited to a few key sources.
- And we are still missing key data on prevalence – this is key to understanding other aspects of cyber crime i.e. costs.
- Other key gaps across thematic areas in published evidence around:
  - cyber offenders
  - costs of cyber crime
  - effectiveness of interventions
- The international element of cyber crime presents particular challenges.

5) Main challenges with the cyber evidence base

- Lack of recording mechanisms that distinguish between online and offline crimes.
- Evidence dispersed across a wide variety of sources and disciplines. Lack of high quality UK-specific evidence.
- Under-reporting of cyber crimes amongst the public and businesses.
- Lack of clarity regarding when some incidents become ‘crimes’ (HOCR requirements).
- Inconsistencies and ambiguity around the measurement and definition of cyber crime across sources.
- Transparency and comparability issues amongst industry sources – particularly in terms of definitions and data used.
- Few high quality population and business surveys available.
- Key survey sources available do not currently distinguish between actual ‘crimes’ and ‘negative online incidents’ (e.g. CSEW).

6) Improving measurement of different types of cyber crime is critical

The following improvements (amongst others) will be needed:

- Systematically improving the quality and range of individual measures of cyber crime. The HO has already:
    - introduced Action Fraud for centralised reporting and recording of fraud and financially motivated cyber crime;
    - introduced a voluntary cyber 'flag' onto PRC;
    - been exploring ways to amend the CSEW questions to focus more on 'crimes' than negative incidents; and
    - been exploring new survey questions e.g. MCS, CVS.
- The HO is setting up a new external working group to help direct the necessary work to improve measures of the cost of cyber crime.
- Further engagement and partnership with private sector business and industry partners (including AV providers) who hold potentially valuable data on cyber crime is also key.

Questions?

Full publication available at:

https://www.gov.uk/government/publications/cyber-crime-a-review-of-the-evidence

Contact:

Samantha.Dowling1@homeoffice.gsi.gov.uk