The Information
Society Alliance
EURIM

Information Society Alliance – Workshop E
Parliament & the Internet Conference, 14th October 2010,
14:15-15:15, Room R, Portcullis House, Palace of Westminster

Chair: Rt. Hon Alun Michael MP
Rapporteur: Dan Mount (EURIM)

SUMMARY OF MAIN POINTS:

1) The messages of “Race Online” and “GetSafeOnline” need to be merged in a simple message of “How to be confident and safe online”.

2) We need to know what we know *and what we don’t really know* about the scale and impact of cybercrimes and quantify and tackle the links between fraud, cybercrime and organised crime, domestic and international, across public and private spheres.

3) There may be no consistent pattern about who benefits the most from public-private partnerships: but perhaps all that matters is that ‘both/multiple parties’ benefit. Not every party will benefit from each initiative.

4) The private sector can gain if public authorities do not just *collect their* intelligence about crimes against business but also *use* this to deal *jointly* with threats.

5) Parts of the business sector must be seen as ‘deserving victims’ and as co-preventers.

6) The volume of fraud cases is at an all-time high and over 50% of consumers say they have been victims of fraud, at some level, over the past 12 months.

7) We need to understand individuals’ susceptibility to fraud and target the right people at the right time with the right messages. 80 – 90% of consumers now use anti-virus software and there is a need for behavioural change in attitudes and approaches to online transactions and social networking.

8) We will only succeed if we work together, build networks of organisations and experts, benchmark and sharing best practice, focusing on information sharing and prevention and delivering co-ordinated messages to the public.

NOTE OF MEETING DISCUSSION

1. Rt. Hon Alun Michael MP

1.1. Alun Michael welcomed those attending the workshop and gave an overview of the structure of the session which would open with a presentation by Dr. Michael Levi (Professor of Criminology at Cardiff University), followed by Alexandra Moore (National Fraud Authority) and Tony Neate (GetSafeOnline).

2. Dr. Michael Levi

2.1. Dr. Levi set out what he saw as being the steps towards better e-crime management, which necessarily must include the mapping of cybercrime problems and the ways they are combated. Dr. Levi is currently carrying out a scoping exercise which will form the basis of a comprehensive audit of the e-crime policy space.

2.2. **Framework Assumptions:** Organised crimes, frauds and terrorism – cyber-enabled or not - are shaped by and respond to the environments provided by the licit world: private & public sectors, plus law enforcement. This calls for rethinking traditional divisions of interest into 'public' and 'private' since they are interdependent but not identical. National boundaries are unhelpful for problem identification and solution, but they are still an essential jurisdictional basis for public sector and some private sector bodies.

2.3. **Key Points:** We need to know what we know *and don't really know* about the scale and impact of cybercrimes. There may be no consistent pattern about who benefits the most from public-private partnerships: but perhaps all that matters is that 'both/multiple parties' benefit. Not every party will benefit from each initiative – have to see this as a process that develops over time (like the Wolfsberg private banks and their AML initiatives)

The private sector can gain if public authorities do not just *collect their* intelligence about crimes against business but also *use* this to deal *jointly* with threats – parts of the business sector must be seen as 'deserving victims' and as co-preventers.

2.4. The Need for Audit:

- Confusion/struggles over labelling of acts.
- Identity theft is often better described as 'identity duplication'.
- Same act as damage, espionage, fraud, play, theft, warfare.
- Elision of threat and manifest harm.
- What are our knowledge gaps about different types of cyber-risks & how are they likely to change over time?
- *Can* we sensibly predict more than short-term trends in risks?
- How and in what terms do we measure cyber-harms?
- Is there any reason to think that some measures are better?
- How are we *actually* organised (a) to prevent and (b) to deal reactively with cyber-harms?
- How do we measure our individual and collective impact on cyber-harms, and can we do this better?
- How would we know that things were getting better or worse?

2.5. Research Design (Phase 1 – Secondary Data collection, duration 3 months).

Rapid Evidence Assessment (REA) of published academic and industry research and Government reports on the prevalence and impact of cybercrime:

- British Crime Survey.
- Information Security Breaches Survey (BIS).
- Former NHTCU/NOP surveys.
- Audit Commission surveys.
- British Chambers of Commerce surveys.
- Federation of Small Businesses surveys.
- CIFAS & UKPA reports.
- Symantec/Cybersource/other industry reports.

Collation and analysis of official offence data from police databases:

- Home Office
- SOCA
- Constabularies
- Central e-Crime Unit
- Action Fraud/NFIB

2.6. Research Design (Phase 2 – Primary Data Collection).

Interviews on perceptions of the cybercrime problem and mapping cybercrime control:

- Policy makers.
- Criminal justice and security agencies.
- Industry partners.
- Academic experts.

Need information on what people want and expect to give and to receive from other parties, and how satisfied they are.

Online Delphi Group focused on establishing a partnership approach to controlling cybercrime.

2.7. Research and Design (Phase 3 – Analysis and Research).

This would involve the production of a preliminary position paper which could then be circulated for responses/advance reactions before the final report is compiled. This would allow us to put together an e-crime reduction model which could challenge the current distribution of resources (and powers).

3. Rt. Hon Alun Michael MP

3.1. We hope that those present will offer their constructive comments on: what we can offer, what we might do, and what we could do….etc.

4. Alexandra Moore (National Fraud Authority)

4.1. The NFA is increasingly focussing on fraud prevention. Fraud is generally increasing. KPMG barometer report suggests the volume of fraud cases going through the courts is currently at a 21 year high. Fear of fraud is also on the increase with over 50% of consumers having been victims of fraud (at some level) over the last 12 months.

4.2. Scale of Fraud in the UK:

- Highest private sector loss = financial services industry: £3.8bn/$5.8bn (12%).
- Largest public sector fraud loss = tax & benefits systems.
- £3.5bn committed against individuals and charities (at least).
- £2.7bn due to ID crime.
- £9bn linked to serious organised crime.
- Latest UK fraud loss estimate: £30.5bn/$47bn.

4.3. Impact on victims:

- Victims find reporting fraud confusing and embarrassing.
- Can cause extreme stress, bankruptcy, even suicide.
- Fraudsters are sophisticated and organised.
- Victims are often the most vulnerable.
- Fraud is under-reported, often “silent”.

4.4. UK National Fraud Strategy (4 key priorities):

- Building and sharing knowledge and intelligence in relation to fraud.
- Setting clear priorities for action.
- Raising awareness and standards of victim support.
- Ensuring activity is sustainable and bolstering the UK’s long term protection against fraud.

4.5. Agencies/initiatives implementing the National Fraud Strategy:

- Action Fraud.
- National Lead Force.
- National Fraud Intelligence Bureau.
- National Fraud Authority.

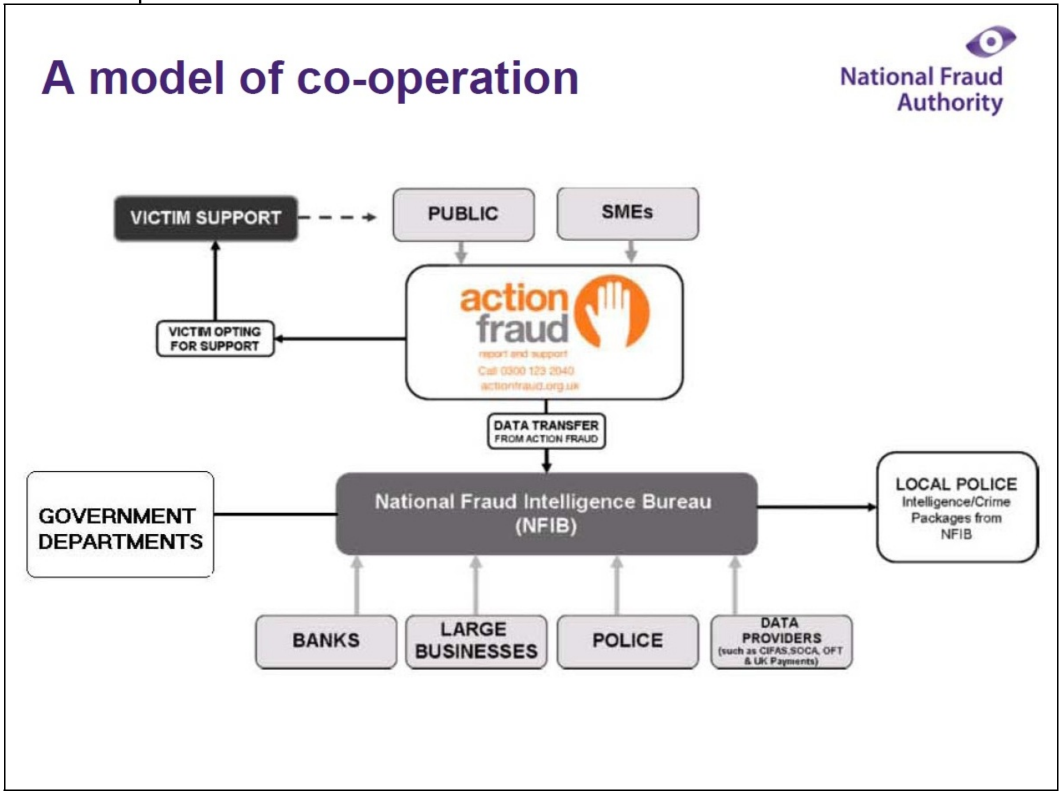
4.6. Action Fraud (contact centre and online reporting portal):

- Run by National Fraud Authority.
- For individuals and SMEs.
- Provides up-to-date advice, guidance and support.
- Gathers reports of confirmed and attempted fraud crime.
- Feeds into crime packages for investigation + intelligence packages.

4.7. Better Intelligence:

- 70,000 contacts to Action Fraud in past 3 months.
- Over 5,000 crime reports with average fraud loss £500.
- 44% reports are of e-enabled fraud (online shopping/auction fraud + dating scams).
- Exposure of scam online clothing website 2010 after > £1m ($1.51m) worth of goods never delivered.
- Proactive prevention: Action Fraud online alerts to advise and encourage self protection.

4.8. A model of co-operation:



A model of co-operation

National Fraud Authority

VICTIM SUPPORT

PUBLIC

SMEs

action fraud
report and support
Call 0300 123 2040
actionfraud.org.uk

VICTIM OPTING FOR SUPPORT

DATA TRANSFER FROM ACTION FRAUD

GOVERNMENT DEPARTMENTS

National Fraud Intelligence Bureau (NFIB)

LOCAL POLICE
Intelligence/Crime Packages from NFIB

BANKS

LARGE BUSINESSES

POLICE

DATA PROVIDERS
(such as CIFAS,SOCA, OFT & UK Payments)

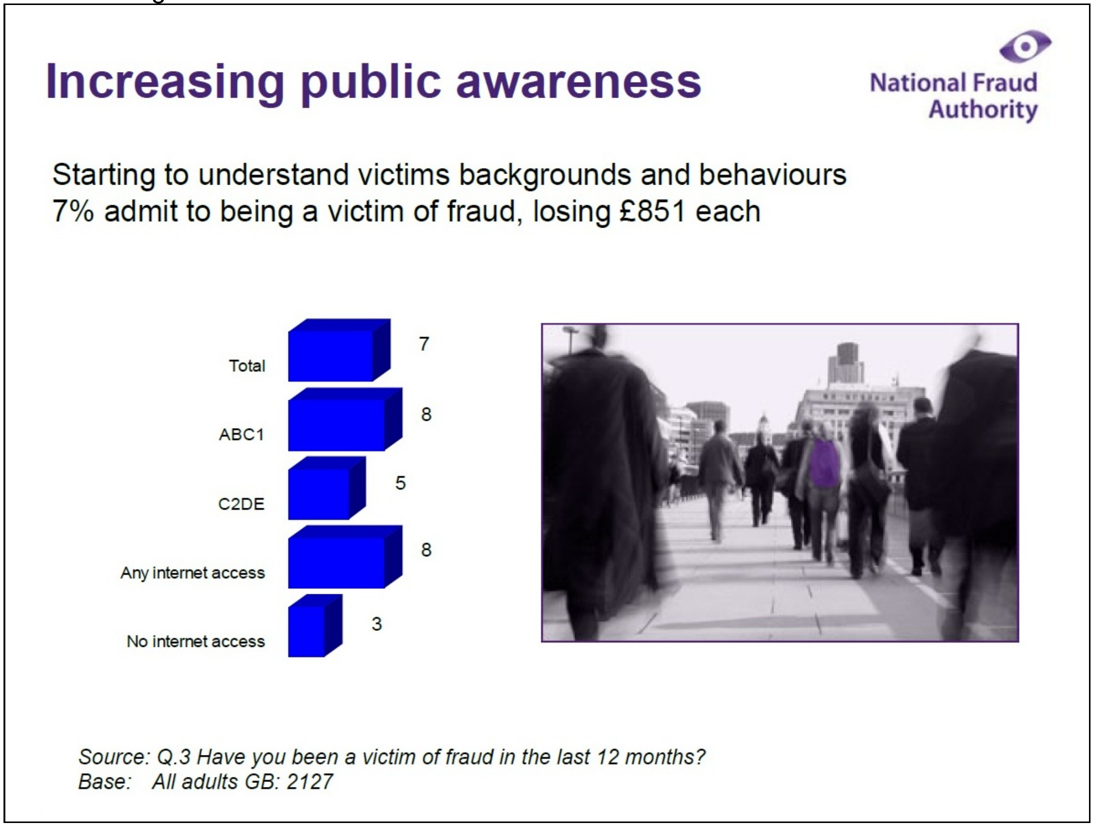
4.9. A model for intelligence sharing – NFA Information Sharing Taskforce:

- Public/private sector joint working to improve info sharing.
- Significant financial services representation.
- Identifies priority blockages.
- Shares effective solutions.
- Resolves or escalates issues.

4.10. Targeting ID crime:

- 85,000 victims of impersonation fraud and 24,000 victims of takeover fraud.
- Key enabler for financial fraud & terrorism.
- NFA led strategic threat assessment with key Govt bodies, police and private sector.
- Resulting strategy recommended specific interventions to detect, disrupt and deter criminals.
- Now, boosting response: reducing criminals' access to genuine identity information.
- Increasing barriers to obtaining genuine travel documents & licences.
- National ID Fraud Awareness Week – new ID crime figure.

4.11. Increasing Public Awareness:



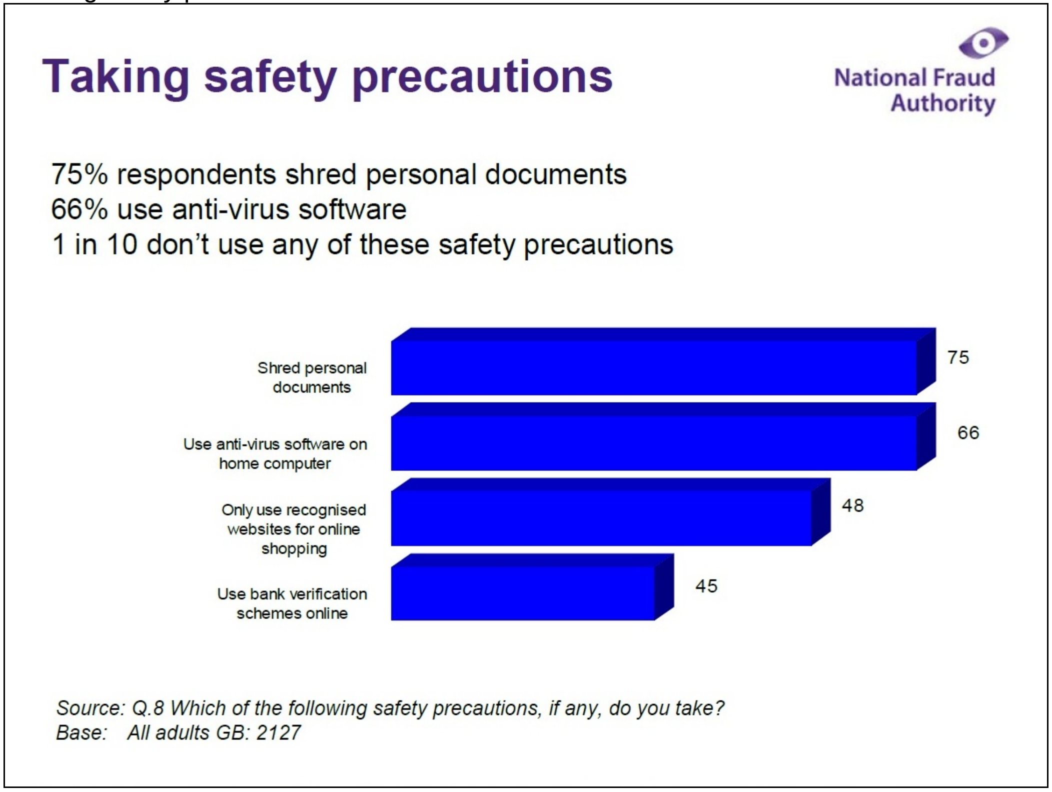
Increasing public awareness

National Fraud Authority

Starting to understand victims backgrounds and behaviours
7% admit to being a victim of fraud, losing £851 each

Source: Q.3 Have you been a victim of fraud in the last 12 months?
Base: All adults GB: 2127

4.12. Taking safety precautions:



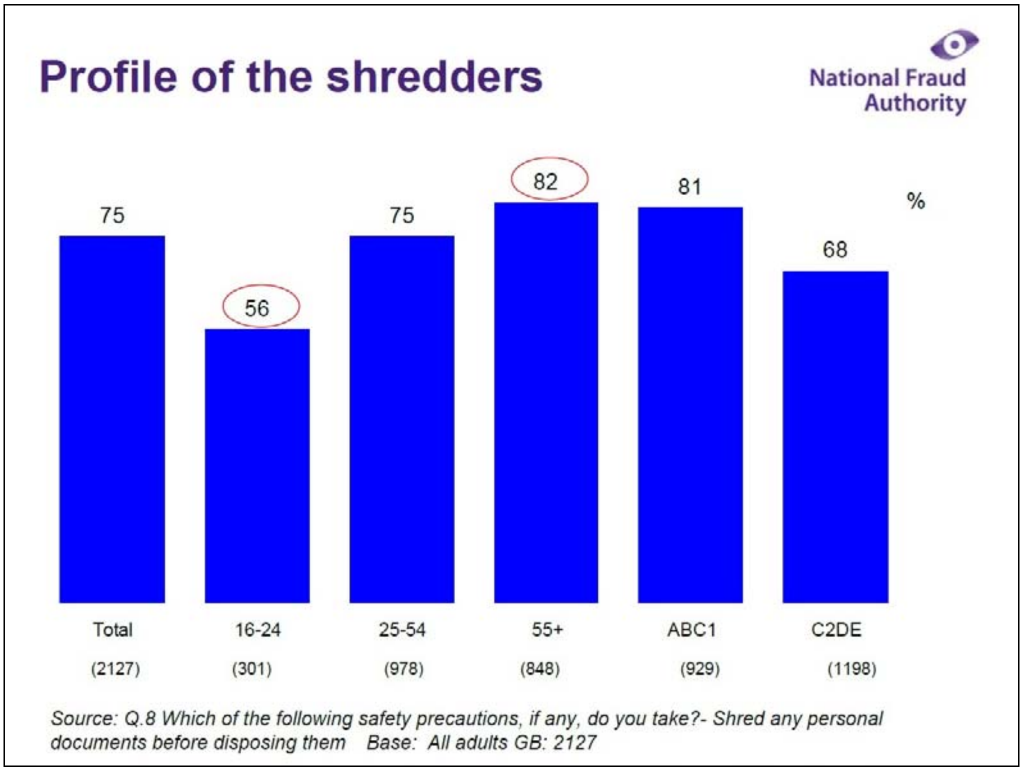
Taking safety precautions

National Fraud Authority

75% respondents shred personal documents
66% use anti-virus software
1 in 10 don't use any of these safety precautions

Source: Q.8 Which of the following safety precautions, if any, do you take?
Base: All adults GB: 2127

4.13. Profile of Shredders:

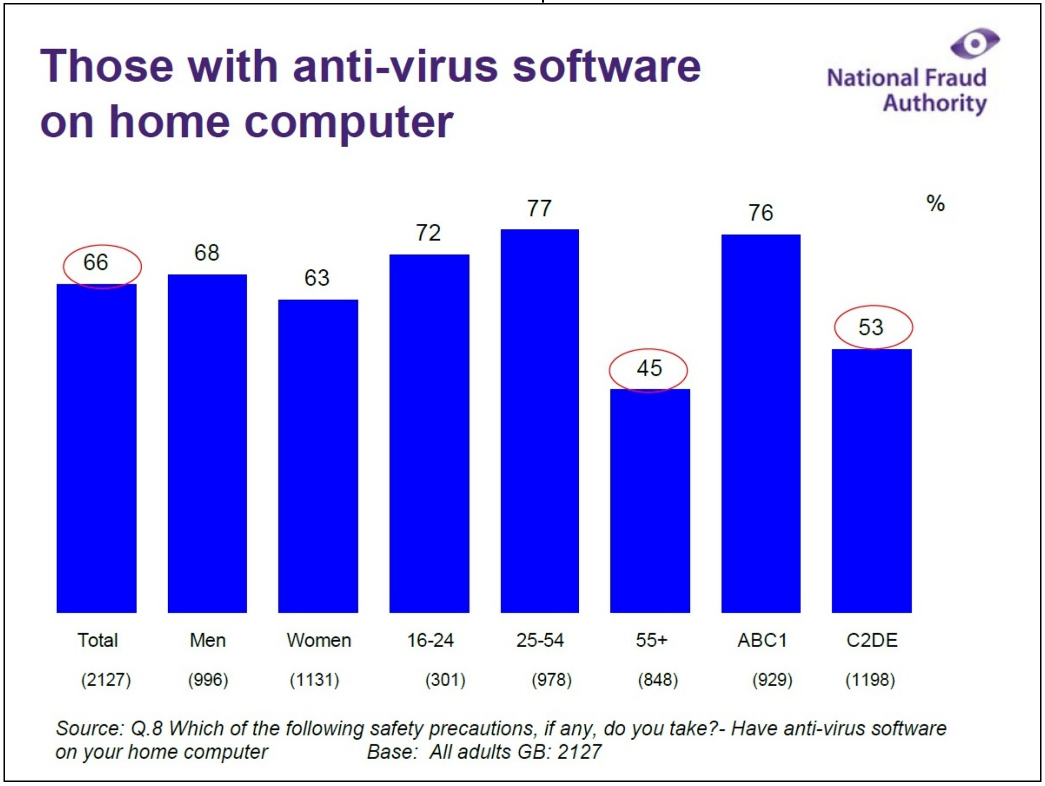


Profile of the shredders

National Fraud Authority

Source: Q.8 Which of the following safety precautions, if any, do you take?- Shred any personal documents before disposing them Base: All adults GB: 2127

4.14. Those with anti-virus software on home computer:

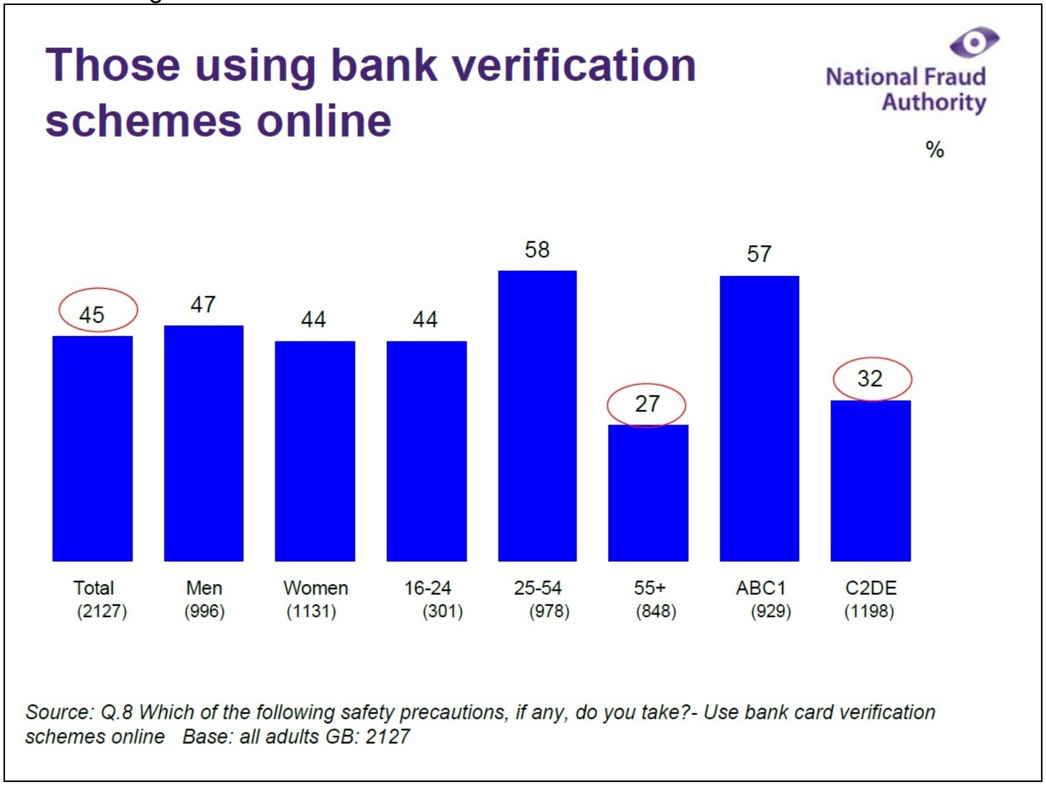


Those with anti-virus software on home computer

National Fraud Authority

Source: Q.8 Which of the following safety precautions, if any, do you take?- Have anti-virus software on your home computer Base: All adults GB: 2127

4.15. Those using online bank verification schemes:



Those using bank verification schemes online

National Fraud Authority

Source: Q.8 Which of the following safety precautions, if any, do you take?- Use bank card verification schemes online Base: all adults GB: 2127

4.16. So what next? The single most powerful tool to dilute the fraud threat to individuals is to increase their awareness and knowledge and empower them to self protect – and by doing so changing their attitudes and behaviours.

4.17. Segmentation – understand individuals' susceptibility to fraud. There are common triggers – both emotional and rational drivers can affect attitudes and behaviour. The interplay between attitudinal and behavioural dimensions helps us understand and evaluate susceptibility to fraud. The approach needs to be to positively influence these dimensions to effect measurable change in the vulnerability and susceptibility of individuals. This also needs to be applied across the relevant sectors by our partners. The key to success in this instance is to target the right people at the right time with the right messages.

4.18. Fighting fraud together:

- We will only succeed if we work together.
- Build networks of counter-fraud organisations & experts.
- Benchmark and share best practice.
- Recognise, quantify and tackle links between fraud and organised crime, and fraud and cyber crime, both domestic and international, and across the public and private spheres.
- Focus on information sharing and prevention.
- Co-ordinated messages to the public.

5. Tony Neate (Managing Director - GetSafeOnline)

5.1. GetSafeOnline is the UK's leading source of unbiased, user-friendly advice about online safety for consumers and smaller businesses. It is supported by HM Government, the Serious Organised Crime Agency (SOCA) and leading businesses in the UK. It advises and educates individuals and smaller businesses on how to use the internet safely and securely.

5.2. Things have already improved in many areas. For example 5-6 years ago 40-50% of consumers used anti-virus software. Now this figure has risen to 80-90%. As a result GetSafeOnline now concentrates its efforts on aiding consumers and businesses to "protect themselves" now that most people are aware of the potential risks involved.

5.3. There is a need for a behavioural change across consumers in their attitudes and approaches to online transactions and social networking.

5.4. There have been 50,000 hits on the GetSafeOnline website this year – 15% up on last year.

5.5. GetSafeOnline undertakes 4-5 major initiatives/campaigns every year including the GetSafeOnline Summit (to be held this year on the 15th of November at BIS Conference Centre).

6. Subsequent questions and general discussion (unattributed):

6.1. Alun Michael called on those present to add to these approaches.

6.2. GetSafeOnline and its awareness campaigns and initiatives are central to safety in this area; it is disappointing that there are not more companies involved.

6.3. It was remarked that Martha Lane Fox's initiative didn't have enough big brands on board and that perhaps if GetSafeOnline joined forces with that campaign the two operations could attract more companies to participate.

6.4. Fraud affects the willingness of people going online. A recent Oxford Internet Institute survey suggests that people who regularly use the internet are not put off using it by negative experiences. Can further evidence be collected to support this?

6.5. The way messages about danger are communicated is important. Negative campaigns tend to discourage those who are not online – perhaps it would better to adopt a “green cross code” approach?

6.6. The internet is also a force for good as it helps rapidly spread awareness about new online scams.

6.7. To the previous generation “spam” and “cookies” had a different meaning. Language can sometimes be more of a barrier and a force for alienation than the technology itself.

6.8. 70,000 enquiries to the National Fraud Authority is a phenomenal number of contacts. Are a lot of these enquiries relating to common sense issues or technical issues?

RESPONSE (Alexandra Moore): there is usually a mix of different enquiries. Some focus on the common sense side of things, others are more scam specific.

6.9. Most people are not suspicious enough online.

6.10. There are a wide range of different places to report e-Crime – for example GetSafeOnline, Know the Net, Action Fraud….etc. Should access to these be channelled through some kind of primary first port of call web portal to streamline the experience for consumers?

6.11. No one expects to receive their bank card and their PIN number in the same envelope from their bank. The public in this instance have been educated as to what industry standard of behaviour to expect. We need to apply similar industry standards in the online world – and there is a burden on industry to evolve these.

6.12. How much information do people really expose? In an environment where people will accept facebook friend requests from people they do not know – there is a certain burden on the consumer to apply a common sense approach in protecting their data.

6.13. The internet is an international space so this clearly requires an international solution, not just national initiatives.

6.14. There is a penchant in the media for focusing on negative internet news stories rather than positive ones.

6.15. The UK is the most advance e-commerce nation in the world. 10 pence in every pound is currently spent online. We need this sector to work in a safe and accessible manner which supports consumer and business engagement with online activity.