National Audit Office

MEMORANDUM BY THE
NATIONAL AUDIT OFFICE
FEBRUARY 2010

Staying Safe Online

Our vision is to help the nation spend wisely.

We promote the highest standards in financial management and reporting, the proper conduct of public business and beneficial change in the provision of public services.

The National Audit Office scrutinises public spending on behalf of Parliament. The Comptroller and Auditor General, Amyas Morse, is an Officer of the House of Commons. He is the head of the National Audit Office which employs some 900 staff. He and the National Audit Office are totally independent of Government. He certifies the accounts of all Government departments and a wide range of other public sector bodies; and he has statutory authority to report to Parliament on the economy, efficiency and effectiveness with which departments and other bodies have used their resources.

Our work leads to savings and other efficiency gains worth many millions of pounds; at least £9 for every £1 spent running the Office.

Contents

The National Audit Office study team consisted of:

Jo James, Robert Cook, Erica Bertolotto, Claire Hardy and Alan Broadhead under the direction of Aileen Murphie.

This report can be found on the National Audit Office website at www.nao.org.uk

For further information about the National Audit Office please contact:

National Audit Office
Press Office
157-197 Buckingham Palace Road
Victoria
London
SW1W 9SP

Tel: 020 7798 7400

Email: enquiries@nao.gsi.gov.uk

Summary

1 The internet is integral to modern life, providing easier access to information, larger markets with more choice for consumers and more opportunities for social interaction. 70 per cent of people use the internet[1], particularly for email and for obtaining information. As part of its Digital Britain strategy, the Government is investing £200 million in fast broadband services to enable more people to benefit from improved access.

2 There are significant economic benefits to Government and businesses, as well as additional convenience for the public, from increasing the take-up of online services. However, the internet also provides more opportunities for criminals. It enables them to commit traditional crimes such as theft or fraud in new and more sophisticated ways, but also to commit new crimes such as the generation of malicious codes to attack the IT systems of citizens, businesses, and government. The internet also gives sexual predators a new means to access children and the impact of e-enabled harm on children is immeasurable.

3 People will be deterred from using online services if they do not feel safe and secure online. Internet users need appropriate protective software loaded on their computers, but they also need to be aware of good practice which will help to protect their data. For example, significant risks arise from sharing personal information which can be used to commit fraud.

4 On average 11-16 year olds spend 2.5 hours a day online[2], and younger children are becoming regular and confident internet users. Three quarters of 11-16 year olds use instant messaging to communicate with friends and 62 per cent use the internet for doing homework[3]. Using wireless technology, young people can access the internet almost anywhere – and away from parental supervision and guidance. Young people need to protect themselves from the risks that the internet presents in terms of grooming for sexual abuse and exposure to inappropriate content, as well as harassment and bullying.

1 Oxford institute, the internet in Britain 2009 and Ofcom accessing the internet at home 2009

2 NAO survey of 1700 children and young people April 2009

3 NAO survey of 1700 children and young people April 2009

5 Responsibilities for raising awareness of internet security measures, to help protect children and adults, are spread across a range of Government bodies including the Home Office, Department for Children, Schools and Families, the Serious Organised Crime Agency (SOCA) and the Child Exploitation and Online Protection Centre (CEOP). The Cabinet Office is responsible for information assurance strategy and direction across Government (**Figure 1** overleaf).

6 This report focuses on two specific initiatives: Get Safe Online and ThinkuKnow:

- **Get Safe Online** is an industry-public partnership providing internet security advice and information to adults and small businesses. Total funding in 2008-09 (which covers staffing and administration as well as website hosting and management) was £578,747 (after deduction of VAT), including a Government contribution of £150,000 paid by the Cabinet Office. It receives no cash funding from the Serious Organised Crime Agency (SOCA), but its steering group is chaired by a former member of the National Hi-Tech Crime Unit, who is now employed by SOCA;
- **ThinkuKnow**, which is an initiative to improve child safety online, is run and funded by the Child Exploitation and Online Protection Centre (CEOP), as an adjunct to its wider remit to tackle child sex abuse and exploitation as well as helping to bringing offenders to justice. Funding in 2008-09 (excluding accommodation and overheads borne by CEOP) amounted to £666,562, about half of which was through the European Union.

7 We examined whether the initiatives provide the advice that internet users need and their effectiveness in changing people's behaviour. Our research included interviews, review of documents and qualitative research with 1200 adults, 1000 small businesses and 1700 children (Annex One).

Figure 1

Government departments referred to in this report

Cabinet Office	Co-ordinates policy and strategy across government departments.
	Due to publish the Cyber Security Strategy in early 2010
	Provides £150,000 per year for Get Safe Online and is a steering group and board member.
Department for Business, Innovation and Skills	From early 1990s to 2008 commissioned biennial surveys into security breaches amongst businesses
	The former Department of Innovation, Universities and Skills (now part of the Department for Business, Innovation and Skills) partnered with the Trades Union Congress and Get Safe Online to launch a toolkit to improve workers' internet security awareness and skills
	Get Safe Online steering group member.
Department for Children, Schools and Families	Provides online practical guidance and advice for parents and carers on use of the internet.
	Jointly with Home Office, set up the UK Council for Child Internet Safety in 2008 to coordinate the work of public, private and third sector organisations to facilitate a more holistic approach to child safety online.
Department for Culture, Media and Sport	Published Digital Britain (June 2009) on strengthening and modernising the UK's digital infrastructure.
Home Office	Set up Internet Task Force on Child Protection which was instrumental in setting up ThinkuKnow.
	Funds police via Police Authorities and Serious Organised Crime Agency
	Published Extending Our Reach: A Comprehensive Approach to Tackling Serious Organised Crime, July 2009 and expected to publish an e-crime strategy in December 2009.
	Get Safe Online steering group member.
Serious Organised Crime Agency (SOCA)	Intelligence-led law enforcement agency sponsored by but operationally independent of the Home Office tasked with reducing the harm caused by serious organised crime including e-crime and hi-tech crime.
	Provides staff support for Get Safe Online events.
Child Exploitation and Online Protection Centre (CEOP)	Accountable through SOCA but operationally independent of it, CEOP is part of UK policing. CEOP is dedicated to protecting children on and offline, in partnership with industry, charities and global law enforcement.
	Responsible for ThinkuKnow programme for schools and other educational institutions, and web-based resources for children, parents and teachers.

Source: National Audit Office

Key findings

On the effectiveness of Get Safe Online providing advice to adults and businesses (Part 1)

8 Get Safe Online has made the most of limited funding to promote its messages to large numbers of people. Our research found that, when prompted, 11 per cent of small business and 11 per cent of adults were aware of Get Safe Online as a source of advice[4]. Targeted marketing, through organisations such as the Student Loans Company and Age Concern, has also enabled it to reach vulnerable groups.

9 Our research indicated that following viewing the Get Safe Online website there were some specific examples of improved confidence and security awareness, particularly among older internet users. People who explored the site in detail and who were less confident or knowledgeable about internet security found the advice to be informative and reassuring.

10 Get Safe Online is dependent upon leveraging industry support. Lower than expected numbers of sponsors and uncertainty about the timing of payments has reduced its ability to deliver core activities over the last year and action is needed to ensure its longer-term sustainability.

11 The public is presented with a wide range of advice on use of the internet from many different websites provided by Government, industry, the third sector and others. Get Safe Online is perceived as a one-stop-shop for internet security advice for adults and businesses. However, we found 17 distinct areas of Government websites with information about internet security, only six of which included links to Get Safe Online, demonstrating a lack of co-ordination of effort across Government. There is a risk that, without such co-ordination, the information provided may not be consistent and up to date and that there will be a duplication of effort in providing advice.

On the effectiveness of ThinkuKnow at reaching children and their parents (Part 2)

12 CEOP is well-placed to offer advice to young people because of its criminal investigation role. Children and teachers were very positive about the quality of the materials provided.

[4] NAO survey of 1200 adults, April and May 2009

13 Our research indicated that awareness of the need not to divulge personal data had improved following ThinkuKnow training. Nevertheless, we found that 5 per cent of children were still willing to meet face-to-face alone with someone that they only know online; CEOP believes that this is a considerable improvement over recent years. Children who have had ThinkuKnow training were more likely to know what to do if they are threatened online and were very unlikely to do nothing.

14 CEOP's cascade approach to training ambassadors and trainers has enabled ThinkuKnow programmes to be delivered to 4 million children cost-effectively. But it does not enable CEOP to monitor the quality of training delivered. CEOP recognises that it now needs to target those geographical areas with lower or no take-up of training.

15 The UK Council for Child Internet Safety (UKCCIS) was established in 2008 following publication of the independent review by Dr Tanya Byron into child internet safety. It consists of representatives from Government and law enforcement organisations, charities, education and industry. One of its aims is to raise awareness of e-safety issues among children, young people, parents and other adults through a public information and awareness campaign. Exactly how the roles of UKCCIS and CEOP (with its crime investigation and ThinkuKnow education roles) will ultimately fit together is still being debated. However, in November 2009, UKCCIS and CEOP agreed that CEOP will host a "one-stop-shop" landing page for the UK Government addressing all child internet safety issues.

Conclusion

16 Our conclusion is an overall judgement against the following criteria:

- whether Government initiatives to provide internet safety advice meet the needs of internet users; i.e., do they provide the right advice to the right people?
- whether these initiatives are effective in changing public behaviour.

17 In terms of creating opportunities for reaching large numbers of people with their messages, Get Safe Online and ThinkuKnow have achieved very good value for their limited resources, using cost-effective means to disseminate advice.

18 It has not so far been possible to measure whether the two initiatives represent value for money in terms of changing public behaviour on a significant scale. Both Get Safe Online and CEOP lack data on who they have reached and consider that comprehensive evaluation is beyond their resources. Our research suggests that both initiatives have produced some effective materials, but that there is scope for improvements and further tailoring to particular audiences.

19 The stability of Get Safe Online is dependent upon the financial commitment of sponsors. Between 2006 and 2009, the number of sponsors remained the same, but the amount of sponsorship declined. Against this backdrop, Get Safe Online did well to maintain its website, marketing and the annual "GSO week", but the funding position poses risks. Shortly after its successful GSO week in November 2009, Get Safe Online hosted a luncheon event for 40 potential sponsors and other interested organisations, and is now in discussion with several companies about becoming sponsors. A solid commitment from government would help to assure the longer term sustainability of the initiative. ThinkuKnow's funding platform is stronger, but relies on project-based EU grants, at some cost in flexibility, cost efficiency and long term assurance. Strong cross-government cooperation is essential to promoting public awareness on both sets of issues and will continue to be a priority in development of the forthcoming e-crime and UKCCIS strategies.

Recommendations

a. **Raising people's awareness of internet security and confidence in using the internet has potentially wide benefits for citizens and the public sector. The Government and Get Safe Online sponsors make an annual commitment to fund the initiative, which means that Get Safe Online is unable to commit resources to plan for longer than the coming financial year**. Government should work with Get Safe Online to identify a mechanism for providing more stable, predictable and adequate finance. It should simultaneously encourage the adoption of a medium-term strategy, outlining options depending on the level of funding available. Such a plan may make it easier for potential investors to see how their sponsorship will make a difference.

b. **A number of different Government-sponsored organisations aim to support internet users to be secure. These include Get Safe Online, the Police Central E-crime Unit, the National Fraud Reporting Centre, bodies which conduct research related to internet security and all Government websites providing the public with relevant advice. There are clear risks of duplication of effort, confusing advice and failure to share information.** Government should minimise these risks by synchronising responsibilities and putting in place clear protocols for coordinating different initiatives to ensure joined-up research, advice, reporting and law-enforcement. Government departments should promote Get Safe Online and ThinkuKnow as sources of advice on preventing e-crime on their websites, through displaying their logos, or live streaming content. This would also help improve brand recognition and encourage people to view the advice provided.

c. **Get Safe Online collects information on the reach of its campaign but it does not collect evidence on the effectiveness of its advice in changing the behaviour of target groups. This limits its ability to prove or refine the effectiveness of its advice – and potential sponsors are looking for firm evidence of the impact from their investments**. Government should use its influence in Get Safe Online to prioritise a proportion of medium term expenditure for user testing and monitoring the take-up by different groups. Simultaneously, Government should coordinate other research efforts to support detailed identification of those most vulnerable to particular internet security threats and those who lack confidence in their internet security.

d. **The UK Council for Child Internet Safety (UKCCIS) is seeking to coordinate the efforts of all its members. Proposals include a coordinated research strategy and a one-stop-shop for advice for parents**. Since the completion of this audit CEOP and UKCCIS agreed that the CEOP website will be used as a one-stop-shop for parents and children. UKCCIS and CEOP should consider how best to develop this approach to coordinate and target their activities to ensure that children, parents and teachers get the advice they need, and know where to find it. Their activities should be dovetailed to minimise the risk of duplication with each organisation concentrating on its own area of comparative advantage.

e. **CEOP's cascade approach to training trainers has been particularly effective in delivering ThinkuKnow to large numbers of children. CEOP now recognises the need to improve its data on training delivered and systems for measuring quality of delivery**. CEOP should implement those changes so that it is able to monitor and target those areas and schools with low take up and ensure that all ThinkuKnow materials are tested for their effectiveness in changing behaviour. This is likely to entail resource costs but ultimately has the potential to improve the effectiveness of ThinkuKnow.

Part One

Advice for adults and businesses provided by Get Safe Online

1.1 Get Safe Online, which was created in October 2005, describes itself as the "UK's leading source of unbiased, user-friendly advice about online safety for consumers and smaller businesses". It has always been a joint Government-industry partnership, with the Government contributing £150,000 annually from Cabinet Office (**Figure 2**). Responsibilities for raising awareness of internet security measures are spread across a range of Government bodies. The Serious Organised Crime Agency (SOCA) provides staff to help with the annual "GSO Week" (conferences, media events and workshops). The Steering Group, on which Home Office is also represented, is chaired by a former National Hi-Tech Crime Unit officer who is now a member of SOCA.

Figure 2

Key facts about Get Safe Online

Remit and aims

- raise internet security among consumers and small businesses;
- build trust and increased confidence in their ability to transact safely;
- enable growth of online activity

Funding and institutional arrangements

- Cabinet Office funding: £150,000 annually
- Total budget 2008-2009: £578,747 (including £353,747 from private sector sponsorship and £75,000 from Ofcom).
- Get Safe Online is a Company Limited by Guarantee. All decisions are taken by a Steering Committee, comprised of private and Government sponsors.

Means of delivery

- Advice provided via the website www.getsafeonline.org
- Marketing campaign to promote security messages and
- direct people to the website. This includes an annual "GSO week" (comprising a one day conference and various media events), road shows, conferences and workshops.

Source: National Audit Office

Get Safe Online has made the most of limited funding to promote its key messages

1.2 Get Safe Online has used a range of different means to promote its key messages, including national, regional, online, and specialist media, and an annual 'Get Safe Online week'. Our survey showed that when prompted, 11 per cent of adults and 11 per cent of small businesses had heard of Get Safe Online[5]. Adults were aware of it through the internet or the television and businesses had usually heard of it by word of mouth (**Figure 3** overleaf). Awareness was particularly high among businesses that had some experience of e-enabled crime, and among younger adults. Sixteen per cent of parents of young children were aware of Get Safe Online.

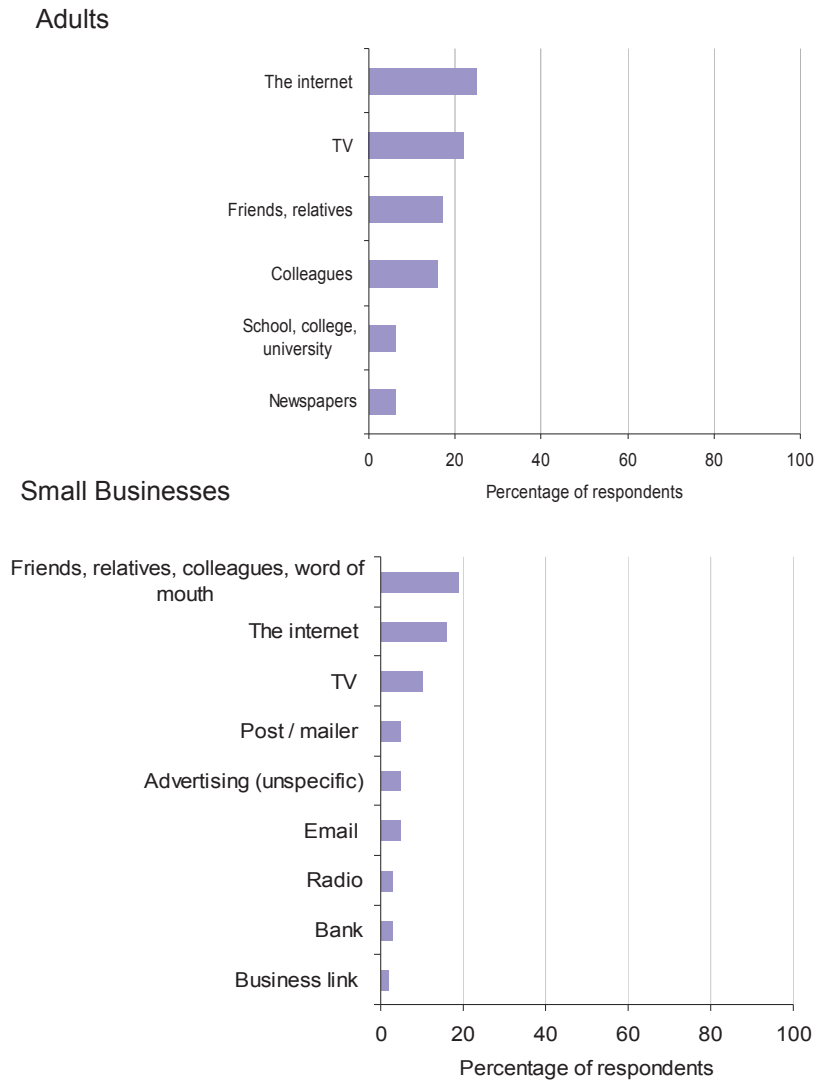
1.3 Get Safe Online has made good use of targeted marketing to increase its profile among those people most vulnerable to fraud by channelling marketing through specific organisations. By including leaflets with letters from the Student Loans Company, it made contact with over one million students in each of 2007 and 2008. Get Safe Online also supported the Office of Fair Training's scams awareness month in February and partnered Age Concern and Help the Aged.

1.4 Get Safe Online has maintained its website and successfully increased numbers of visits since its launch (**Figure 4** on page 19). Analysis of web statistics indicates that there are over 605,000 links to the Get Safe Online website - far more than its US counterpart, Staysafeonline, with 25,000 links. Shortly after GSO Week in 2008, monthly visits to the website increased from an average of 55,000 per month to 90,000 suggesting that such promotional activity generates additional interest in the website. The increasing length of time spent on the website, which Get Safe Online aims to increase from an average 1.75 to 2.5 minutes, also suggests that people find it useful.

[5] NAO survey of 1200 adults April and May 2009

Figure 3

Survey responses on sources of awareness of Get Safe Online



Source National Audit Office survey of 127 adults and 110 businesses aware of Get Safe Online, April 2009

Figure 4

Key deliveries of Get Safe Online

Key deliveries	Estimated number of people reached		
	2007-08	**2008-09**	**2009-10 on target to reach**
Website visitors (average monthly)	52,147	32,352	75,000
Page views	139	171	205
Average time on site (minutes)	1.52	1.57	2.05
Blog visits (average monthly)	--	2500	5000

Source :Get Safe Online

1.5 Our user testing of Get Safe Online suggested that it was effective in increasing awareness of internet security issues. Most businesses found the 'Advice for small businesses' section comprehensive, useful and informative. Adult users gave positive feedback on the "dictionary" function and the 'How safe are you?' assessment quiz (**Figure 5 and Figure 6** overleaf).

Figure 5

Views on Get Safe Online's website

Get Safe Online's website was well received by most adult users:

"It's very clear, easy to understand because people want things in a normal language they can understand, because it doesn't use long words for people who don't understand them." *(Female, Newcastle depth interview. Unwary and heavy-user of the internet)*

"The cartoon makes it friendly." (Female, London focus group. Wary and light user of the internet)

… **but heavier and more confident internet users were more likely to think that Get Safe Online was not targeted to them**:

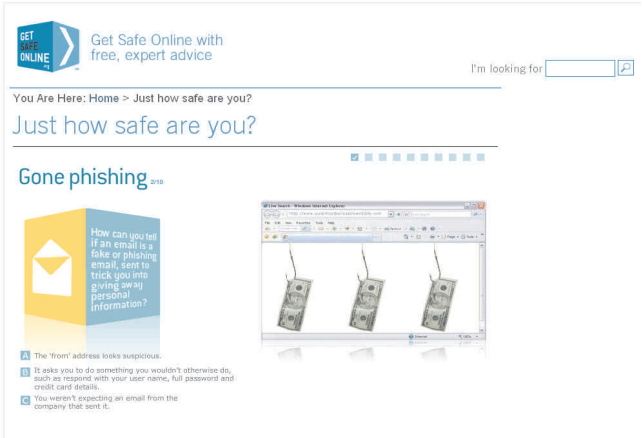
"I think it would be more useful for older people, like my mum and dad." (Young male, unwary, heavy internet user)

"It doesn't really attract me. I sort of lose interest, because there are so many websites you can go on and find this kind of information*." (Male, unwary and heavy internet user*)

Source: National Audit Office research – focus groups and interviews with 1200 adults, April 2009

Figure 6

Example pages from Get Safe Online website



Source: Get Safe Online

1.6 Our survey[6] and focus group of UK adults found that they were aware of the online threats posed by financial fraud and ID fraud, but the extent of their awareness was often strongly correlated to their confidence in using the internet. Respondents considered that the website and campaign covered the main risks relating to internet-enabled fraud but the majority would like more information on how to implement security measures or advice. People who explored the Get Safe Online website in greater detail and those who are less confident and less knowledgeable about internet security were more positive about the website's usefulness and presentation. Most of the less confident users liked the reassuring and friendly tone of the website.

1.7 User testing of the website has not been a priority for Get Safe Online. We estimate that testing would cost about £30,000. In 2005, Get Safe Online commissioned research to identify four target groups with different internet security needs, but with the exception of a special section for small businesses, has only been able to sustain a one-size-fits-all website. Our user testing found that just over half of those who had revisited the website[7] said that they felt more confident online as a result. This was especially prevalent among older groups where six of seven respondents said that their confidence increased following visiting the website.

[6] National Audit Office survey of 1200 adults April 2009
[7] NAO follow-up interviews with 31 user testing participants

Get Safe Online's impact in changing behaviour

1.8 There is some evidence of improvement in internet users' approach. Get Safe Online's surveys indicated a general increase in take up of all security measures between 2007 and 2008[8]. It is impossible to attribute how much of this may be directly from Get Safe Online's promotional activity and how much arises from other sources of advice. Ten of the 31 people we interviewed following user testing had changed their take-up of security measures or their willingness to disclose personal information (**Figure 7**). Of the 21 who did not change their behaviour, the majority were sophisticated and experienced web users, those who did not make much use of the internet anyway, and younger, more cavalier users. It was older, more wary internet users who made small changes to behaviour.

Figure 7

The impact of Get Safe Online's website on behaviour

People who explored Get Safe Online thoroughly became more confident about their ability to be safe online and expanded the range of activities they carried out online:

"I think I worry less now because…I understand it a lot more now. ….Now that I know what pages to go to for back up and security, I don't feel quite as bad. A friend …said I should be on Facebook because it would make it easier for us to contact each other and send stuff. I went into that and followed the details through. I'm now on Facebook." *(Female, 70+, cautious internet user).*

"The bit under 'Bank on-line safely'…was quite an influence. It makes you more confident about using it… less threatening using the online banking.." *(Male, student, extremely wary internet user)*

Source: National Audit Office Focus groups and interviews

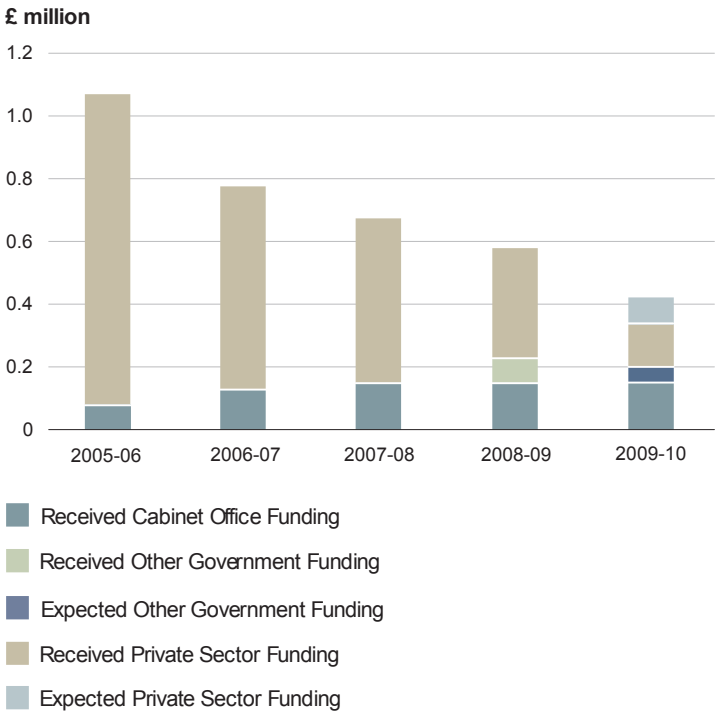
Get Safe Online has concerns over longer term funding

1.9 Get Safe Online has done well to maintain its website, carry out some marketing and promote the annual "GSO Week", although declining funding poses risks for Get Safe Online's longer term sustainability. Cabinet Office and each of the industry sponsors are expected to contribute £150,000, annually. The number of sponsors has remained the same since the year following Get Safe Online's launch, but not all sponsors felt able to commit to the expected level on an ongoing basis. Get Safe Online has accepted lesser contributions from some sponsors, who cited caution in the wake of the recession as the key reason for committing less funding (**Figure 8** overleaf).

[8] Omnibus surveys of 1000 people: take-up of antivirus software had increased from 80 to 85 per cent of respondents, the percentage with firewalls had increased from 80 to 84 per cent. There are small, and not significant, differences from NAO survey results which are due to sampling differences.

Figure 8

Get Safe Online funding has reduced over the period 2005-06 to 2009-10



Source: National Audit Office analysis of Get Safe Online income at the end of January 2010

1.10 Get Safe Online requests that funding be received in time for the start of its financial year on 1 July each year. Between 2006 and 2009, Get Safe Online received Government sponsorship and funds from five private sector sponsors. In each year, three paid within three months of 1 July. As at 31 January 2010, Get Safe Online had received £286, 957 from sponsors for 2009-10 (after VAT has been paid). A further £134,000 is expected within the next few months. As funding is uncertain Get Safe Online has difficulty planning more than a few months in advance and is unable to adopt a medium-term strategy. A three-year plan Get Safe Online commissioned from consultants in 2007 was never adopted because of changing priorities and lower than anticipated funding

1.11 Although GSO Week had taken place every year, Get Safe Online told us that uncertainty about the amount and timing of payments, and a fall in in-kind contributions from private sector backers, has meant that activities have had to be modified on a monthly basis. The scale and scope of GSO Week 2008 was reduced,

with a number of cities cut from the itinerary and workshops cancelled. For 2009, some local community events and promotional activities were cut and other costs had to be re-negotiated.

1.12 In 2009, staff numbers were reduced in line with falls in income. Some staff have been working in excess of their contracted hours pro-bono, devoting much of their time to liaising with and seeking new sponsors.

1.13 The lack of a medium to long term strategy has made it more difficult for Get Safe Online to attract and retain sponsors. Sponsors told us that their decisions on whether or not to renew their support take account of the likely return on their investment and scope for advertising. The economic climate, their perception of Ministerial interest in the initiative, and the lack of a clear "home" for Get Safe Online within Government were further factors.

1.14 The success of Get Safe Online Week 2009, including a keynote address by the Rt Hon Angela Smith MP, has resulted in more positive feedback from sponsors for the coming year. Shortly afterwards, Get Safe Online hosted a luncheon event for 40 potential sponsors and other interested organisations. Get Safe Online is now in discussion with several companies about becoming sponsors.

1.15 The United States and Australian Governments operate initiatives similar to Get Safe Online which are constrained by small budgets and few staff. However, they are both wholly run by relevant Government departments and funded by Government. Although they have not benefited from private sector partnerships, they have had guaranteed, timely funding, supporting longer-term planning[9].

Government involvement in awareness raising activities for adults and businesses

1.16 Get Safe Online is perceived as a one-stop-shop for internet security advice for adults and businesses, but a wide range of advice on use of the internet is available from many different websites provided by Government, industry, the third sector and others. The Government has not yet coordinated its efforts, with the risk that over time the various websites may not all be up-to-date and there may be duplication of effort in providing advice. The National Audit Office found 17 distinct areas of Government websites offering advice on internet safety in addition to that provided by Get Safe Online, only six of which included links to Get Safe Online, demonstrating a lack of co-ordination of effort across Government (**Figure 9** overleaf). There is a risk that, without such co-ordination, the information provided may not be consistent and up to date, and that there will be a duplication of effort in providing advice.

[9] National Audit Office interviews with Stay Smart Online, Australia and OnGuard Online, USA

Figure 9

Examples of areas of government websites which give advice to adults on internet security

Website		Link to Get Safe Online
Home Office		
Staying Safe Online	A list of tips in the crime prevention section on how to stay safe when online.	No
Search and advice Public	Link to PDF of good practice guidance for members of the general public searching online	No
What your business really needs to know	Link to a PDF for small businesses on how to operate safely online	No
Internet Crime	Description of what internet crime entails and what the Home Office has done to prevent it.	No
Metropolitan Police		
Computer crime prevention	A list of key pointers on how to keep your computer safe and a link to “when the chips are down”.	No
When the chips are down	Advice on computer security and access control for home computers with links to more in-depth studies.	No
Direct Gov		
Home and Community	Technical advice for adults with links to further information.	Yes
Identity theft, keeping safe	Advice on the prevention of identity theft with a link to the Home Office website.	No
Department for Business, Innovation and Skills		
What we do consumer factsheets	Links to advice on various topics on consumer issues, fact sheet on internet shopping section.	Yes from some links
Information security: business advice	Advice on how to protect your business from e-enabled crime with links to advice on viruses, inappropriate usage, human resources monitoring and education, unauthorised access theft and systems failure	Yes from some links

Website		Link to Get Safe Online
Consumer Direct		No
Scams – what to look out for	General; advice on avoiding scams which covers internet based scams.	Yes
Online shopping, safe shopping	Detailed advice to consumers on how to shop safely online.	No
Ofcom		No
Media literacy	Portal providing links to a number of Government sites with internet security advice	Yes
City of London Police		
Computer Security	Information on how to protect your computer hardware with a link to a site on illegal online content including child abuse images.	No
Information Commissioners Office		
Topic Specific Guides	Links to advice on specific topics including Junk mail and social networking.	No
Keeping your personal information personal	Advice for young people about how to stay safe online. With specific advice on different areas.	No
Business link		
IT and e-commerce – data protection and your business	Advice on how to protect your business interests online.	Yes

Source: National Audit Office

Part Two

Advice for children and young people and their parents about staying safe online

2.1 ThinkuKnow is an educational initiative run by the Child Exploitation and Online Protection Centre (CEOP) as an integrated part of its child protection work (**Figures 10 and 11**). Its ethos is to help young people have fun online and to make the most of the internet but at the same time teach them how to protect themselves against online threats. It developed from a National Crime Squad pilot initiative to provide internet safety advice in schools ("Getting to Know IT All"), working with Childnet (an internet safety charity) and was delivered by volunteers from Microsoft and local police forces. CEOP, when it was established in 2006, combined this with an education website from the Home Office, re-launching it as the ThinkuKnow programme, with contributions in kind from various private sector and charitable organisations.

Figure 10

Key facts about ThinkuKnow

Remit and aims

- internet safety awareness for children, parents and teachers, particularly on risks relating to child abuse.
- raise awareness of online safety, develop and promote new educational materials and make the internet safer

Funding and institutional arrangements for 2007/2008

- Government funding: £277,366
- European Funding of £389,196
- Total budget: £666,562
- The programme is run by CEOP, as part of its wider remit to tackle child sex abuse and exploitation as well as helping to bringing offenders to justice. CEOP covers overheads including accommodation.

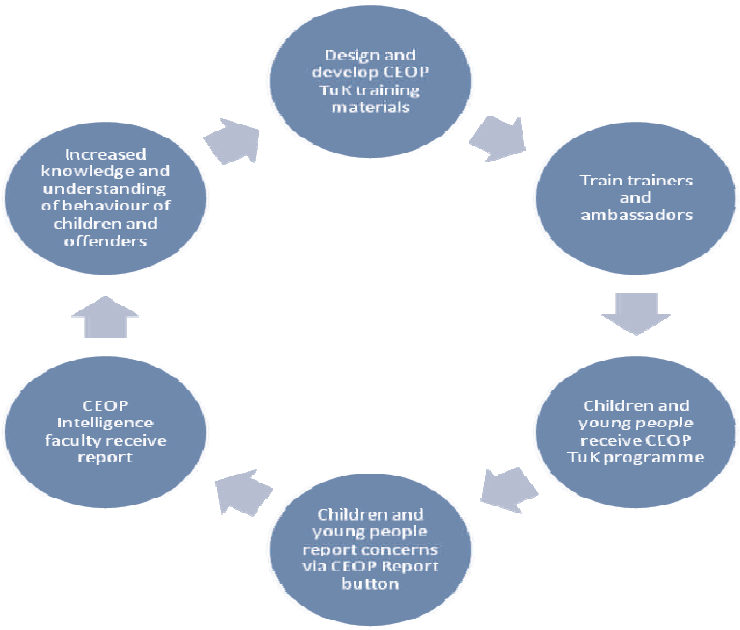
Means of delivery

- training for professionals to deliver presentations with videos to children, often in schools;
- publication of a range of materials for children in different age groups, including booklets and videos;
- a website (www.ThinkuKnow.co.uk) with designated areas specifically for children aged 5-7, 8-10, and 11-16 and for parents/carers and teachers/trainers.

Source: National Audit Office

Figure 11

ThinkuKnow is an integrated element of CEOP's work



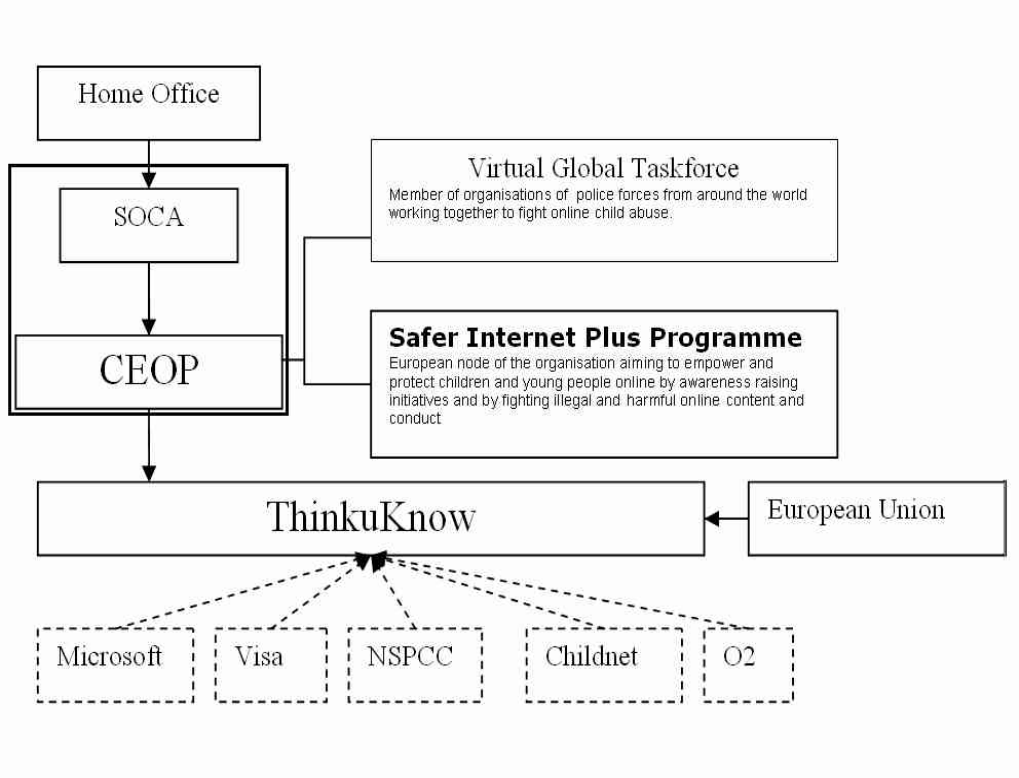
Source: CEOP

Organisation and funding of the ThinkuKnow programme

2.2 ThinkuKnow benefits from staffing and accommodation from CEOP and European funding (**Figures 12 and 13** overleaf); CEOP has become the European node for internet safety advice for children. CEOP told us that the administrative costs of the grant process amount to roughly £100,000 over two years and long lead-in mitigates against flexible programmes that can adapt quickly to changing threats or threat levels.

Figure 12

Organisational and funding arrangements for the ThinkuKnow programme



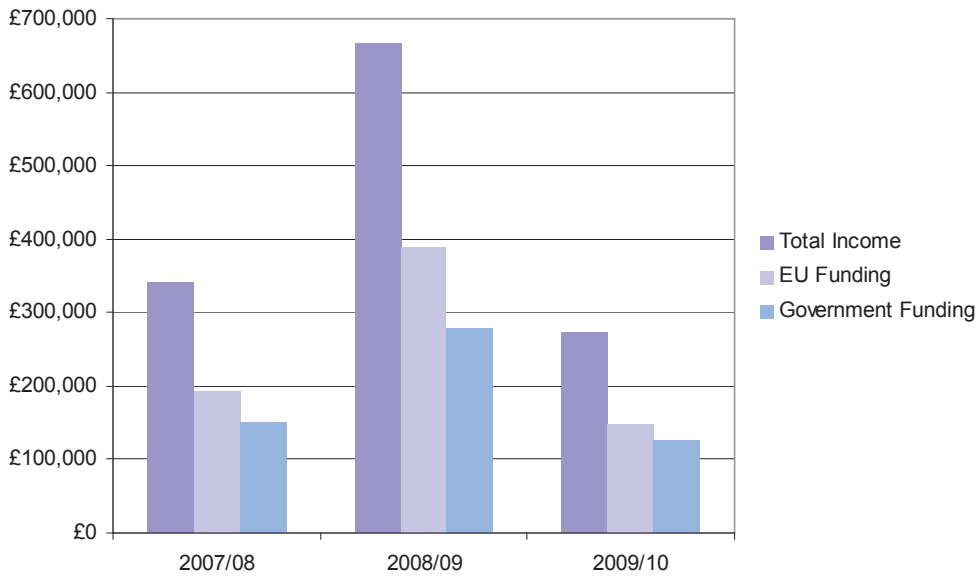
Source: National Audit Office

2.3 CEOP has attracted 23 private sector sponsors across its activities including Microsoft, (who provide technical advice and volunteers), the National Society for Prevention of Cruelty to Children (child protection and policy advice), Childnet, 02 and Visa, who offer help in kind.

2.4 Because of the nature of sexual abuse crimes, children who are victims are especially unlikely to report them. Creation of the "CEOP Report" button which now features prominently on websites used by young people, and which links directly to its investigations team, has enabled CEOP to have a much better understanding of the extent and nature of incidents and adapt its approach to detection, investigation and education accordingly (**Figure 14**).

Figure 13

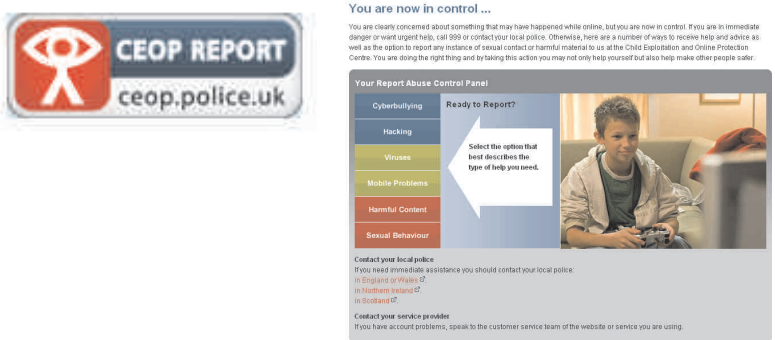
Variation in annual funding applicable to ThinkuKnow



Source: CEOP

Figure 14

The CEOP report button enables young people to report problems they encounter online, including inappropriate sexual contact or behaviour



Source: CEOP

2.5 The UK Council for Child Internet Safety (UKCCIS) was created in 2008 following publication of the independent review by Dr Tanya Byron into child internet safety[10]. Its members include representatives from Government and law enforcement, charities, the education sector and industry, with secretariat support from the Department for Children, Schools and Families. UKCCIS has no remit for crime investigation.

2.6 The Byron Review highlighted that 53 per cent of adults want more and better information about the internet and that 57 per cent of parents whose children use the internet do not know where to get information about how to protect their children online. To help raise awareness of e-safety amongst parents, children and others, the review recommended:

- including e-safety in the Government's major child safety awareness campaign that was to begin in summer 2008;
- working with UKCCIS partners to develop an authoritative one-stop-shop child internet safety website by spring 2009;
- ensuring that Parent Know How funded help lines are able to signpost parents concerned about e-safety to sources of further information by autumn 2008; and
- working with CEOP and other Council members to launch an e-safety week in 2009.

2.7 It is not yet clear to us how the roles of UKCCIS and CEOP will ultimately fit together. The Byron Review acknowledged that there would be "an inevitable overlap between work to address illegal activity and work to address online content, contact and conduct which is potentially harmful and inappropriate." The challenge will be to provide an internet interface for advice and reporting on all issues related to child internet safety, without undermining the work already in place. The recent decision that UKCCIS will use the CEOP website as its portal on child internet safety is a welcome clarification.

CEOP is making progress against its targets for ThinkuKnow

2.8 ThinkuKnow has reached large numbers of children, through its training programme in schools and its website but it has had limited success in reaching parents (**Figure 15**). Targets have been achieved by using a cascade model, whereby CEOP has provided half-day training sessions for professionals working with children[11] and trained "ambassadors", who are qualified to deliver half-day training to other professionals.

[10] Safer Children in a Digital World, Dr Tanya Bryon, March 2008

[11] Individuals can register with ThinkuKnow if they can demonstrate that they already work in some capacity with children and are Criminal Records Bureau Cleared. All those registered can give some training to children, including videos in assembly, but to deliver the full programme need to be ThinkuKnow trained.

Figure 15

ThinkuKnow's performance against targets

Target (2008-09)	Progress as at September 2009
During the academic years 2007/08 and 2008/09 3.5 million UK children aged between 7 and 16 will have the ThinkuKnow programme delivered to them.	Achieved. CEOP estimates that 3.6 million children have received the programme.
By the end of July 2009 to provide every UK primary school with ThinkuKnow resources underpinned by online and offline advice and support.	Achieved. Information leaflets distributed to every primary school in the United Kingdom.
During 2007/08 and 2008/09 deliver a public awareness campaign aimed at engaging with 5 million UK parents and carers.	Not clear. Records showed delivery to only 20,134 parents in May 2009, but CEOP is collating information which more accurately reflects interactions with parents. NAO research indicates that 7 per cent, of parents of children aged five to eighteen were aware of ThinkuKnow in May 2009. This is approximately 680,000 parents in the UK[12].

NOTES

Targets are set as part of the procedure for securing European funding

Source: National Audit Office

2.9 Reflecting its focus on delivering training programmes, CEOP measures its performance based on extent of direct contact with children. It is reliant on performance information provided by trainers, and is currently working with trainers to improve the quality of data it receives from them. Our survey of 71 trainers showed discrepancies between their recollection of deliveries and the data held by CEOP, reflecting that while the self-reporting system is more cost effective, it brings potential for error. (Following further research, CEOP believes that there is under-reporting of training given.) In addition, nine respondents (an eighth of our sample) were recorded by CEOP as not having received training which they claimed to have received.

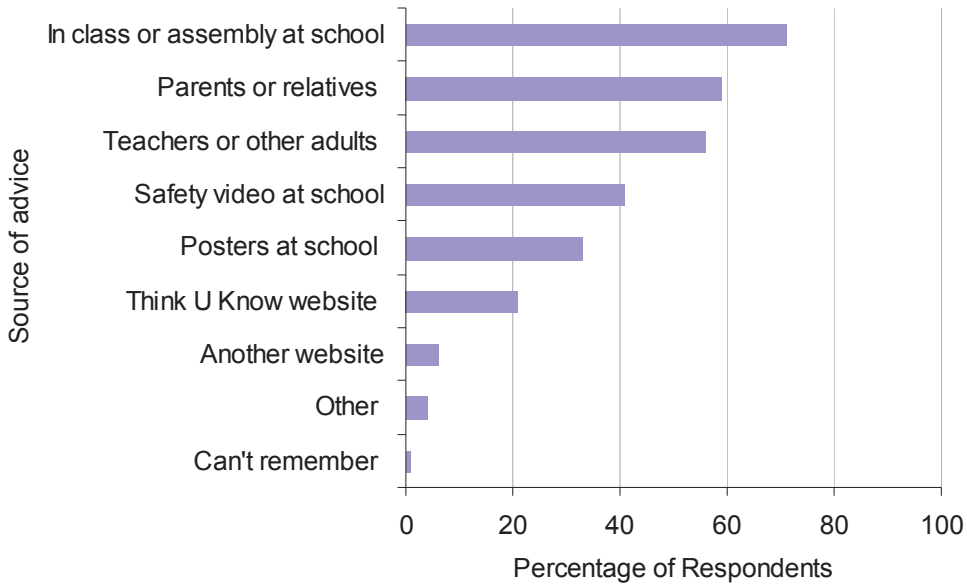
2.10 CEOP aspires to reach all children with its programme. It has sent materials to all primary schools, but does not have the authority or resources to monitor or record which individual children have received the programme. Locations provided by trainers on registration suggest much higher participation among faith-based and independent schools. CEOP recognises that it now needs to target those areas with lower take up, and those schools which have not yet been involved at all.

[12] This is based on 7% of an estimated 10,054,408 parents in the UK, calculated from the NAO survey of 1702 adults over the age of 15.

2.11 CEOP has had limited success reaching its target of engaging with 5 million parents. Parents and relatives are important because they were a commonly cited source of internet safety advice for children, second only to schools (**Figure 16**). Ofcom's 2007 research indicated that 57 per cent of parents whose children used the internet did not know where to go for information on how to keep children safe online[13]. Follow-up research indicated that parents were aware of a range of dangers online, but not all the potential dangers[14]. CEOP is keen to engage more with parents, particularly through encouraging ambassadors to liaise with schools and to run events, for example, at parents' evenings.

Figure 16

Sources of internet safety advice received by children



Source: National Audit Office survey of 1200 children, April/May 2009

[13] Children, Young People and Online Content, October 2007 in Ofcom's response to the Byron Review Annex 5: The Evidence Base – The Views of Children, Young People and Parents Submission date: 30 November 2007

[14] Department for Children, Schools and Families: Parents and Internet Safety – Report from HCI Discussion Groups, May 2009

ThinkuKnow training and materials are well received

2.12 The content and quality of CEOP's training courses for professionals wishing to become ThinkuKnow ambassadors or trainers was highly rated, with 88 per cent of attendees indicating that they were very satisfied or satisfied with the quality of instruction[15]. As a result, all of them felt confident delivering the training to children.

2.13 CEOP does not yet have a mechanism to assess the quality of training delivered by its ambassadors and trainers. CEOP has recently updated its risk register to include quality control. It plans to introduce better qualitative performance measures, a quality assurance programme and a new diploma qualification for its trained Ambassadors. CEOP's records indicated that 706 trainers had provided training to 11-16 year olds without having first had the CEOP specialist coaching[16]. This represents a small proportion of those who are delivering ThinkuKnow training, all of whom CEOP ensures are Criminal Records Bureau checked and already work with young people in some capacity. One third of those responding to emails from us confirmed that they had delivered the programme without this coaching.

2.14 Industry experts and professionals registered with ThinkuKnow rated materials highly, with some videos being regarded as excellent – several have won international awards. Almost all of the 35 professionals we interviewed who had used ThinkuKnow materials were very satisfied or satisfied with the quality and comprehensiveness of materials. The main concern – which CEOP is now addressing - was the absence of materials for young people with special educational needs.

2.15 Amongst children, the ThinkuKnow brand was not particularly well known - children found it difficult to recall if they had received ThinkuKnow training. In one school, where it had been given to all children, only 39 per cent recalled the programme's branding, creating a potential problem for CEOP when they come to evaluate the programme. However, this does not mean that the children do not recall the messages.

2.16 Our survey indicated that majority of children who recalled having had ThinkuKnow were positive about the training received[17]. Some of the videos designed to highlight the potential consequences of risky behaviour online were particularly effective in conveying the messages. When they were asked to comment spontaneously on ThinkuKnow 20 per cent said that they felt it had helped them stay safe online, made them think, or made them aware of dangers and nine per cent commented that it helped them to know what to do if they had a problem. Three per cent of children commented that the website could be more interactive and less text heavy (**Figure 17**)[18].

[15] NAO survey of 40 trainers March 2009
[16] CEOP believes that this figure may be overstated, as some may have received training which has not been recorded, and others may have delivered training which does not require specialist coaching.
[17] National Audit Office survey of 1700 children, April 2009
[18] National Audit Office survey of 1700 children, April 2009

Figure 17

Comments from trainers and children about ThinkuKnow

Comments made by ThinkuKnow trainers about the materials

"The secondary materials were hard hitting, but very good"

Some found the videos shocking or sad, but many remembered the content key messages well:

"Yeah the guy who said he was his friend called Jack and he sent him that picture and he said that his name and he was like a 20 year old man"

"I was crying it was so sad. But I learned not to talk to people, they lie to you, they send you a fake picture and then you know not to trust them if you totally don't know them"

Children thought that the website could be more interactive

"It's too much writing and it makes it boring. Get young people to design new parts"

"I think there should be more games, quizzes, simulations etc to see if someone really does know"

Sources: National Audit Office survey of 40 trainers, focus groups with 84 children and young people, and survey of 1700 children between April and May 2009

ThinkuKnow has had some success in influencing behaviour change

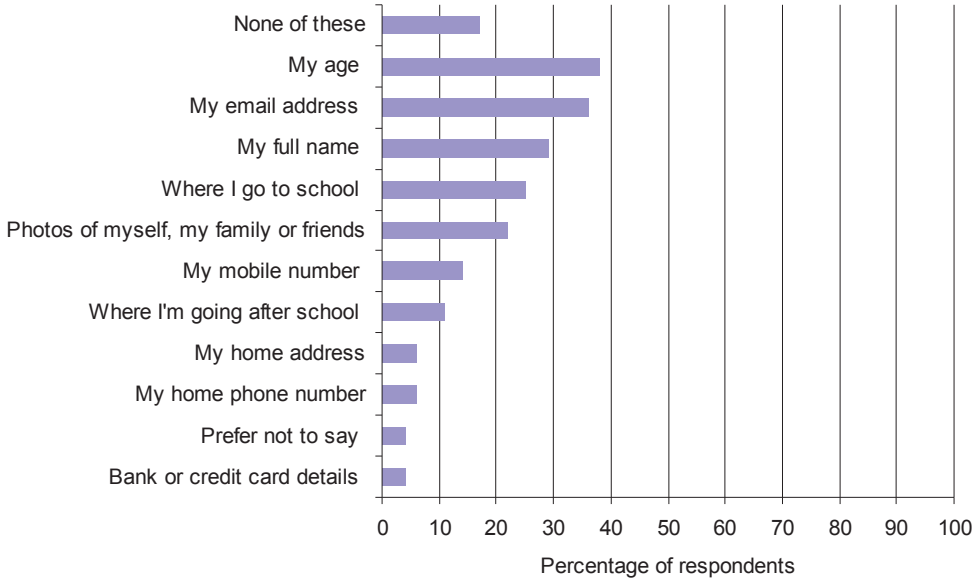
2.17 To help assess the impact of ThinkuKnow training influencing changes in behaviour, we asked 11-16 year old children[19] if they recalled having received the programme and whether they had done certain things in the past (such as sharing a telephone number with a stranger) which they would not do in the future. It is difficult to isolate the impact of the training from other advice received and the differences between reported behaviour before and after training, while they appear positive, were not statistically significant.

2.18 In the past 55 per cent of children had shared some information, such as their age, with someone they had only met online (**Figure 18** overleaf) but our survey suggested that having received safety advice in the last two years reduces the willingness of youngsters to share such information in the future, most prominently their full name, age, school and mobile number (**Figure 19** on page 31). However, these results were not all statistically significant.

[19] Average of children sampled was 13-14 years old

Figure 18

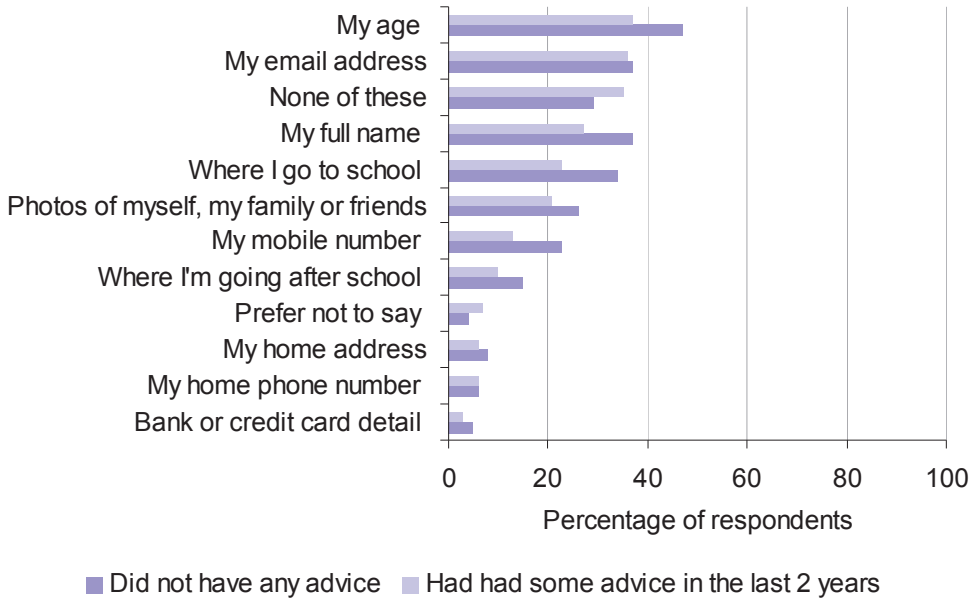
Information shared by child users in the past which could increase vulnerability to harm or abuse



Source: National Audit Office survey of 1700 children, April/May 2009.

Figure 19

Willingness to share information with strangers online by those who have, and those who have not, received safety advice



NOTES

Respondents were told that a stranger was "someone you may have spoken to online for some time, but who you have never met in person"

Source: National Audit Office survey of 1700 children, April/May 2009

2.19 Following ThinkuKnow training young people were very unlikely to do nothing in response to a threatening situation. The majority of those who had received ThinkuKnow were aware that they could report online through ThinkuKnow or Childline.

Annex One

Method	Purpose
Online survey of 1700 children and face-to-face focus groups with young people, April 2009 Administered by the Centre for Abuse and Trauma Studies, Kingston University. 1028 children in ThinkuKnow registered schools and online panel of 690 children. Focus groups in schools registered with ThinkuKnow, commissioned by CEOP.	To explore understanding of ThinkuKnow messages and to look for changes in behaviour. Suggestions from children of how to improve the programme content.
Quantitative survey of 1200 adults (face-to-face) and 1000 small businesses (telephone) and face-to-face qualitative surveys of adults and small businesses, April 2009. The Quantitative survey of adults was representative of the UK population. 2 focus groups of 6 people and 12 face to face, in depth interviews. The survey of Small Business was representative in terms of size, industrial classification and region. A telephone survey of 1000 business, 8 face to face interviews and user testing sessions, followed up 8 weeks later, and 30 telephone interviews.	To test public awareness of Get Safe Online. Awareness of crime committed via the internet, common e-security behaviour and the number of individuals who have fallen victim.
Survey of ThinkuKnow trainers, May 2009 A telephone survey of 71 trainers registered with the ThinkuKnow programme and email survey of 131 ThinkuKnow registered trainers.	To attempt to validate figures collected by ThinkuKnow on child deliveries and assess views on the programme.
Systematic review of documentation on ThinkuKnow and Get Safe Online and semi structured interviews with key staff April 2009.	To understand how the ThinkuKnow and Get Safe Online programmes operate, and the successes and challenges to date.
Systematic review of the literature Review of academic, Government and private sector literature on e-enabled crime and online behaviour carried out by Professor Peter Sommer, London School of Economics.	To understand the scope and scale of e-enabled crime and the online behaviour of the British public.
Email Survey of 706 ThinkuKnow trainers registered as having not received CEOP training, but delivering to secondary level. 131 of the 706 we emailed responded.	To establish if ThinkuKnow trainers had been giving training without the appropriate CEOP coaching.

Telephone Survey of 40 trainers registered with ThinkuKnow.	To gain an understanding of how effective Thinkuknow is from the trainers perspective, and to validate Thinkuknow figures.
Semi structured interviews with: Government and law enforcement: British Educational Communications and Technology Agency Citizens Advice Bureau The Department for Business, Innovation and Skills The Information Commissioner Met Police Central Internet crime Unit National Fraud Authority Office of Fair Trading OFCOM Serious Organised Crime Agency UK Council for Child Internet Safety	To gain an understanding of the role of Government and law enforcement in raising awareness of internet safety.
Third Sector: Childnet Children's Charities Coalition on internet safety Education Advisory Panel Federation of Small Businesses Internet Watch Foundation National Society for Prevention of Cruelty to Children	To gain insight on the third sector's expectations of Government in raising awareness on internet security.
Private Sector: The Association for Payment Clearing Services (now Financial Fraud Action UK) British Bankers Association Cable and Wireless eBay HSBC Microsoft Paypal Symantec	To gain insight on the e-crime threat mad the private sector's expectations of Government in raising awareness on internet security.